(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－200521

(43)公開日　平成10年(1998)７月31日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ
		Ｈ０４Ｌ　9/00	６０１Ｅ

審査請求　未請求　請求項の数15　ＦＤ　外国語出願　（全 77 頁）

(21)出願番号　特願平9－370210

(22)出願日　平成９年(1997)12月24日

(31)優先権主張番号　９６３０９４４４．６

(32)優先日　1996年12月23日

(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　597129263
アイシーオー・サーヴィシーズ・リミテッド
イギリス・Ｗ６・９ＢＮ・ロンドン・クイーン・キャロライン・ストリート・１

(72)発明者　トーマス・フランシス・ジョンストン
イギリス・Ｗ２・６ＤＧ・ロンドン・クリーブランド・スクエア・22Ａ

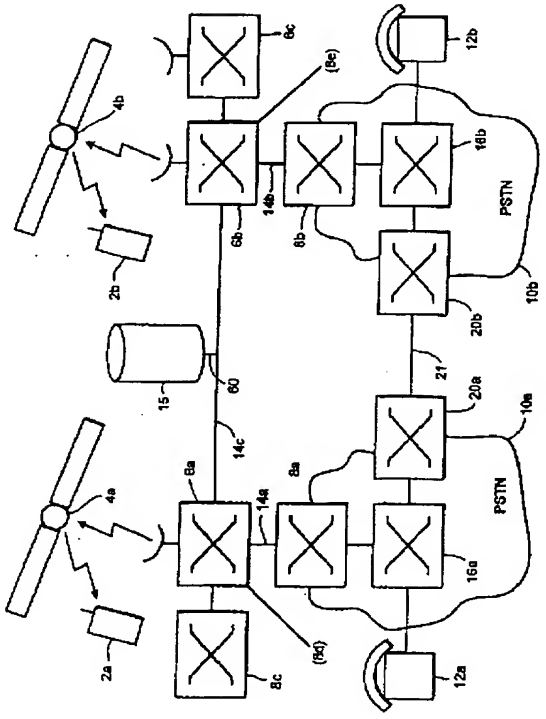
(74)代理人　弁理士　志賀　正武　（外１名）

(54)【発明の名称】　通信保護方法および装置

(57)【要約】

【課題】　複数の端末の間に安全な移動遠距離通信を設定すること。

【解決手段】　本発明は、端末（２ａ，２ｂ）から遠く離れて、第１および第２キー（Ｋａ，Ｋｂ）を記憶し、両方の端末から遠く離れた位置で、第１および第２の個々の部分キー（Ｋｐａ，Ｋｐｂ）を、それぞれ、共通数（ＲＡＮＤ）のマスクされた関数として、かつ、記憶されたキー（Ｋａ，Ｋｂ）のうちの対応するキーとして、生成し、第１部分キー（Ｋｐａ）を個々に第１端末（２ａ）に急送し、第２部分キー（Ｋｐｂ）を第２端末（２ｂ）に個々に急送することを特徴とする。



1

【特許請求の範囲】

【請求項１】　ネットワークを通した端末間の安全なデータ送信を提供するために、第１および第２端末（２a，２b）においてデータを暗号化および解読する際に使用されるべき暗号化キーデータを通信ネットワークを通して分配し、端末は、それぞれ、対応する第１および第２端末キー（Ka，Kb）を記憶する方法において、

端末（２a，２b）から遠く離れて、第１および第２キー（Ka，Kb）を記憶することと、

両方の端末から遠く離れた位置で、第１および第２の個々の部分キー（Kpa，Kpb）を、それぞれ、共通数（ＲＡＮＤ）のマスクされた関数として、かつ、前記記憶されたキー（Ka，Kb）のうちの対応するキーとして、生成することと、

第１部分キー（Kpa）を個々に第１端末（２a）に急送することと、

第２部分キー（Kpb）を第２端末（２b）に個々に急送することとを具備することを特徴とする方法。

【請求項２】　請求項１記載の方法において、

暗号化キーデータは、ネットワークを通した全ての前記端末（２a，２b，２n）の間の同時のデータ送信に対して安全性を提供するために、前記第１および第２端末（２a，２b）および少なくとも１つのさらなる端末（２n）においてデータを暗号化および解読することに対して使用されるべきであり、

端末（２a，２b，２n）から遠く離れて、さらなる端末（２n）の端末キーに対応するさらなるキー（Kn）を記憶することと、

さらなる部分キー（Kpn）を、共通数（ＲＡＮＤ）のマスクされた関数として、かつ、前記遠く離れて記憶されたさらなるキー（Kn）として、生成することと、

さらなる部分キー（Kpn）をさらなる端末（２n）に急送することとをさらに具備することを特徴とする方法。

【請求項３】　請求項２記載の方法において、

端末間のデータ送信が進行中の間に、さらなる端末に対して、端末間のデータ送信に参加させることを具備し、さらなる端末に、端末間のデータ送信に関するタイミングデータを送信することを具備することを特徴とする方法。

【請求項４】　請求項１から請求項３のいずれかに記載の方法において、

前記端末（２）の予め決められたグループ（ＣＵＧ）の端末間の安全な通信を用意するために、前記端末（２）の予め決められたグループ（ＣＵＧ）に対してのみ、前記共通数（ＲＡＮＤ）を伴って前記部分キーを生成することを具備することを特徴とする方法。

【請求項５】　セキュア暗号化コード（KR）に従って、通信ネットワークを通して第２端末（２b）に送信されるべきデータを暗号化するために、個々の端末キー（Ka）を記憶する第１端末（２a）を設定し、データは

2

第２端末（２b）で解読されるべきである方法において、

遠く離れた位置からネットワークを通して第１端末へ急送された部分キー（Kpa）を第１端末で受信し、部分キーは、個々の端末キー（Ka）のマスクされた関数であり、かつ、暗号化コードを決定するための数（ＲＡＮＤ）とであることと、

暗号化コード（KR）を用意するために、受信された部分キー（Kpa）と記憶されたキー（Ka）とを、端末（２a）において比較することとを具備することを特徴とする方法。

【請求項６】　請求項５記載の方法において、

暗号化コード（KR）に従って、第１端末（２a）においてデータを暗号化することと、

暗号化されたデータを、ネットワークを通して、第２端末に送信することとを具備することを特徴とする方法。

【請求項７】　セキュア暗号化コード（KR）に従って、通信ネットワークを通して第１端末から第２端末に送信されるデータを解読するために、個々の端末キー（Kb）を記憶する第２端末を設定し、データは第１端末で暗号化される方法において、

遠く離れた位置からネットワークを通して第２端末へ急送された部分キー（Kpb）を第２端末で受信し、部分キーは、個々の端末キー（Kb）のマスクされた関数であり、かつ、コードを決定するための数（ＲＡＮＤ）とであることと、

第１端末から送信され、かつ、暗号化コード（KR）に従って暗号化されたデータを解読するためのデータ（KR）を用意するために、受信された部分キー（Kpb）と記憶されたキー（Ka）とを、端末において比較することとを具備することを特徴とする方法。

【請求項８】　請求項７記載の方法において、

第１端末から第２端末に送信され、かつ、暗号化コード（KR）に従って暗号化されたデータを、第２端末において解読することを具備することを特徴とする方法。

【請求項９】　請求項１から請求項８のいずれかに記載の方法において、

前記部分キー（Kpa，Kpb，Kpn）またはその各々は、移動通信システムの空中インターフェースを通して、端末（２a，２b，２n）に送信されることを特徴とする方法。

【請求項１０】　請求項９記載の方法において、

空中インターフェースを通して送信されるデータを暗号化することをさらに具備することを特徴とする方法。

【請求項１１】　請求項１０記載の方法において、

個々の端末の端末キーと予め決められたアリゴリズムとを用いて、追加の暗号化を各前記端末において実行することを具備することを特徴とする方法。

【請求項１２】　ネットワークを通した端末間の安全なデータ送信を提供するために、第１および第２端末（２

a，２b）においてデータを暗号化および解読する際に使用されるべき暗号化キーデータを、通信ネットワークを通して分配し、端末は、それぞれ、対応する第１および第２端末キー（Ka，Kb）を記憶する装置（１５）において、
端末（２a，２b）から離れて配置され、端末によって個々に記憶される端末キーに対応する第１および第２端末キー（Ka，Kb）を記憶するデータ記憶装置と、
数（ＲＡＮＤ）を生成する手段と、
個々の第１および第２部分キー（Kpa，Kpb）を、それぞれ、数（ＲＡＮＤ）のマスクされた関数、および、記憶装置に収容された前記キー（Ka，Kb）のうちの対応するキーとして生成する手段と、
第１部分キー（Kpa）を第１端末（２a）に急送し、かつ、第２部分キー（Kpb）を個々に第２端末（２b）に急送するように動作する急送手段とを具備することを特徴とする装置。
【請求項１３】　通信ネットワークを通して、少なくとも１つのさらなる端末と通信する端末（２a，２b，２n）において、
個々の端末キー（Ka）を記憶する記憶手段（ＳＩＭ）を収容する手段と、
個々の端末キー（Ka）のマスクされた関数を具備する部分キー（Kpa）と、前記少なくとも１つのさらなる端末へ共通に送信される数（ＲＡＮＤ）とを、ネットワークから受信し、かつ、暗号化コード（KR）を前記数（ＲＡＮＤ）の関数として生成するために、記憶装置（ＳＩＭ）に記憶された個々のキーを前記部分キーと比較するように動作するキー生成手段（３５a）と、
暗号化コード（KR）に従って、ネットワークを通して送信されたデータを暗号化するように動作する暗号化手段（３７）とを具備することを特徴とする端末。
【請求項１４】　請求項１３記載の端末において、
暗号化手段の動作を選択的に開始する使用者操作手段（３８）を具備することを特徴とする端末。
【請求項１５】　請求項１３または請求項１４のいずれかに記載の端末において、
ネットワークを通して異なるチャネルでデータを送信および受信するように動作し、
暗号化手段（３７）は、第１の前記暗号化コード（KR）に従って、ネットワークを通して送信されるデータを暗号化するように動作し、
第２の異なる前記暗号化コード（KR）に従って、ネットワークを通して受信されたデータを解読するように動作する解読手段（３７）を具備することを特徴とする端末。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、通信ネットワークを通した安全な通信を提供する方法および装置に関する。
【０００２】
【従来の技術および発明が解決しようとする課題】デジタル移動音声通信はよく知られており、かつ、一例はＧＳＭ地上セルラーシステムである。他の例は、インマルサットM衛星電話システム、または、例えば欧州特許公開第０３６５８８５公報に記載されたイリジウム（登録商標）衛星セルラーシステム、または、例えば英国特許公開第２２９５２９６号公報に記載されたＩＣＯ（登録商標）衛星セルラーシステム、または、例えば欧州特許公開第０５１０７８９号公報に記載されたオデッセイ（登録商標）衛星セルラーシステムである。そのようなシステムはワイヤレスリンクを通して動作するので、許可されていない人による（呼の）傍受の危険がある。
【０００３】ＧＳＭシステムは、選択的な暗号計画を具備する。この選択的な暗号計画は、例えば、１９８８年１０月１２日～１４日のデジタルセルラー無線学会（ＤＣＲＣ）において、Deutsche BundespostとFrance TelecomとFernuniversitateとによって出版された学会会報の論文４a”Security aspects and the implementation in the GSM-system”（Peter C.J. van der Arend）に記載されている。さらなる詳細は以下のＧＳＭ勧告において与えられている。
GSM 02.09 ”Security Aspects”
GSM 03.20 ”Security Related Algorithms”
この計画において、識別検証センター（ＡｕＣ）として知られるデータベースは、識別検証サービスへの各加入者に対する個々の暗号化キー番号（Ki）を保持する。この暗号化キー番号（Ki）は、また、加入者の移動端末内に収容された（加入者情報モジュール（ＳＩＭ）として知られる）チップ上に記憶される。加入者は、ＳＩＭ内に記憶されたデータへはアクセスせず、かつ、キーを読み出すことはできない。
【０００４】安全なセッションが要求されると、ランダムな数（ＲＡＮＤ）が、ＡｕＣによって生成され、かつ、暗号化キー（Kc）を計算するために、顧客のキー（Ki）と共に使用される。暗号化キー（Kc）は、セッションの間に、加入者へのメッセージまたは加入者からのメッセージを暗号化および解読するために、使用される。ランダムな数は、ベーストランシーバー局（ＢＴＳ）を介して、ＡｕＣから加入者の移動端末へ送られる。移動端末は、ランダムな数をＳＩＭへ送る。ＳＩＭは、Ａ５と称されるアルゴリズムを使用して、受信されたランダムな数と記憶されたキー（Ki）とから、暗号化キーKcを計算する。故に、ランダムな数は、空中を通して送られるが、顧客のキーKiまたは暗号化キーKcではない。
【０００５】ランダムな数および暗号化キーKcは、ＧＳＭネットワークの基地位置レジスタ（ＨＬＲ）データベース（このデータベースは、関係する加入者に対する

5

詳細を記憶している）へ与えられる。また、ランダムな数および暗号化キーKcは、使用者端末が現在置かれているエリアに対するビジッティング位置レジスタ（ＶＬＲ）へも送られ、かつ、ＢＴＳへ供給される。移動端末は、そのＢＴＳを介して、ネットワークへ通信している

【０００６】移動端末とＢＴＳとの間の空中インターフェースを通して送信されるデータが暗号化されるように、暗号化キーKcは、移動端末とＢＴＳとの両方においてＡ５暗号化アルゴリズムを実行するために、現在のＴＤＭＡフレーム番号と共に使用される。故に、個々の使用者キーKiは、識別検証センターおよびＳＩＭでのみ記憶される。識別検証センターおよびＳＩＭにおいて、暗号化キーKcは、計算され、かつ、ＢＴＳおよび移動端末へ送られる。

【０００７】この計画は、多くの点において十分である一方、空中送信経路を通してのみ保護を提供するので、完全な安全性を提供することができない。故に、ネットワークの固定部分を不正に変更することによって違法アクセスが獲得されることが可能である。従って、端末相互暗号計画が提案されている。暗号化は、ある使用者端末から他の使用者端末へ、空中経路だけでなく、通信経路全体にわたって、実行するので、改善されたプライバシーが得られる。

【０００８】ネットワークを通した通信の端末相互暗号化を提供する際における基本的な問題は、二人の使用者の各々に、同一の、または、それぞれのシークレットキーを提供することにある。ある用途において、１組の端末（例えば、全てが単一の本体によって所有されている）は、全て、同じキーへのアクセスを有する。これは、グループ外部からの人々に対するプライバシーを提供する一方、グループ内の２つの端末間、および、グループ内の３つの端末間の通信に対して、プライバシーを提供しないので、不完全な解決である。

【０００９】公衆キー暗号化システムを使用することができる。このシステムでは、各々の端末は、シークレット解読キーおよび公開暗号化キーを有する。それによって、全ての他のパーティは、データを暗号化するために、暗号化キーを使用することができるが、受取人だけが、公衆暗号化キーを使用して暗号化されたデータを解読できる。

【００１０】全ての使用者がそのような１対のキーを提供されている通信システムが予見され得る。そして、１対の使用者の間の通信が設定される際に、各々は、その解読キーを秘密にする一方で、相手にその暗号化キーを送る。しかしながら、遠距離通信ネットワーク上のそのような技術の使用が、犯罪者またはテロリストに対して、管理の如何なる可能性からも解放された完全に安全な通信を使用して通信することを許可する、という公衆に広まった関心事が存在する。

【００１１】遠く離れた「信頼された第３者の」データ

6

ベースにキーを保持することが提案されている。そのような設備の一例は、”Security measures in communicationnetworks”（K. Presttun：電気通信，１９８６年第６０巻第１号第６３頁～７０頁）に記載されている。２人の使用者（使用者Ａと使用者Ｂ）に対するキーは、遠距離キー分配センターから、共通のマスクされたメッセージとして、分配される。このメッセージは、最初に使用者Ａへ送られる。使用者Ａにおいて、使用者Ａに対するキーは取り出される。そして、使用者Ｂにキーを提供するために、使用者Ａから使用者Ｂに送られる。

【００１２】英国特許出願第９６１１４１１．１号（および、対応米国特許出願番号第０８／８６６９１２号）には、端末相互暗号化および解読計画が記載されている。この端末相互暗号化および解読計画において、端末内に記憶されている端末キーは、遠く離れた「信頼された第３者の」データベース内に追加的に保持される。第１端末と第２端末との間に暗号化された送信を設定するために、各々の端末は、遠く離れた位置から、部分キーが提供される。この部分キーは、データベース内に記憶されたデータから生じる（他の端末の）キーに関するマスクされたデータを含む。その結果、両方の端末は、データが提供され得る。このデータは、端末に記憶されたそれ自身のキーと組み合わさって、端末のそれぞれに対し、共通のシークレットコードを設定することを許可する。このシークレットコードは、ネットワークを通した端末相互暗号化および解読に対して使用され得る。

【００１３】３または４以上の端末の間に安全な電話会議を設定することが望まれる場合、先の参照の「信頼された第３者の」データベースに関する困難性が生じる。部分キーおよび最終暗号化コードが（参加者の数に依存して）長くかつ厄介になる結果、各端末がそれぞれ共通コードを確定できるように、各端末は、電話会議に参加している他の端末の全てのキーに関するマスクされたデータを提供される必要がある。また、コードが（長い部分キーから）盗聴によって確認されるというリスクが増加する。

【００１４】

【課題を解決するための手段】本発明は、これらの問題に対する解決を提供する。本発明は、ネットワークを通した端末間の安全なデータ送信を提供するために、第１および第２端末（２a，２b）においてデータを暗号化および解読する際に使用されるべき暗号化キーデータを通信ネットワークを通して分配し、端末は、それぞれ、対応する第１および第２端末キー（Ka，Kb）を記憶する方法において、端末（２a，２b）から遠く離れて、第１および第２キー（Ka，Kb）を記憶することと、両方の端末から遠く離れた位置で、第１および第２の個々の部分キー（Kpa，Kpb）を、それぞれ、共通数（ＲＡＮＤ）のマスクされた関数として、かつ、前記記憶されたキー（Ka，Kb）のうちの対応するキーとして、生成す

ることと、第１部分キー（Kpa）を個々に第１端末（２a）に急送することと、第２部分キー（Kpb）を第２端末（２b）に個々に急送することとを具備することを特徴とする方法を提供する。

【００１５】本発明は、また、安全な暗号化コードに従って、通信ネットワークを通して第２端末へ送信されるべきデータを暗号化するために、個々の端末キーを記憶する第１端末を設定する方法を提供する。第２端末において、そのデータは、解読され得る。本発明は、遠く離れた位置からネットワークを通して第１端末に急送された部分キーを第１端末において受信することと、暗号化コードを提供するために、端末において、受信された部分キーと記憶されたキーとを比較することとを具備する。部分キーは、個別の端末キーのマスクされた関数であり、かつ、暗号化コードを決定するための数である。

【００１６】本発明は、また、安全な暗号化コードに従って、通信ネットワークを通して第１端末から第２端末へ送信されるべきデータを解読するために、個々の端末キーを記憶する第２端末を設定する方法に拡張する。第１端末において、そのデータは、暗号化される。本発明は、遠く離れた位置からネットワークを通して第２端末に急送された部分キーを第２端末において受信することと、コードを解読するためのデータを提供するために、第２端末において、受信された部分キーと記憶されたキーとを比較することとを具備する。部分キーは、個別の端末キーのマスクされた関数であり、かつ、コードを決定するための数である。

【００１７】故に、本発明によれば、各端末は、他の端末のキーに対する必要なしに、遠く離れた位置から、端末それ自身の端末キーに関するマスクされたデータを含む部分キーを提供される。そのため、プロトコルは、部分キーを長くすることなしに、２つの端末間の通信から電話会議における多数の端末へと速やかに拡張され得る。

【００１８】通常の２つのパーティの呼を３つのパーティの電話会議に拡張するために、または、電話会議内のパーティの数を増加するために、呼が進行中の間に、１または２以上の追加の端末が呼に参加してもよい。この目的のために、参加しているパーティは、該パーティがコードを決定できるように、そのキーのマスクされたバージョンを、パーティ間で続いているデータ送信のためのフレーム番号と共に送られる。それによって、参加しているパーティは、送信されたデータの流れに参加できる。

【００１９】本発明は、衛星移動デジタル通信システムにおける使用に対して予見され、また、対応する地上デジタル移動通信システムにおいて（例えば、ＧＳＭシステムのようなセルラーシステムにおいて）、または、固定リンク通信システムにおいて有用である。本発明は、また、電子メールまたはインターネットのような蓄積送信通信システムで実行されてもよい。

【００２０】

【発明の実施の形態】本発明の実施形態は、添付図面を参照して、一例のみによって、ここに記載される。添付図面は以下の通りである。図１は、本発明を具体化する通信システムの構成要素を概要的に示すブロック図である。図２は、本発明を伴った使用に適した移動端末装置の構成要素を概要的に示すブロック図である。図３は、図１の実施形態の一部を形成する地球局ノードの構成要素を概要的に示すブロック図である。図４は、図１の実施形態の一部を形成するゲートウエー局の構成要素を概要的に示すブロック図である。図５は、図１の実施形態の一部を形成するデータベース局の構成要素を概要的に示すブロック図である。図６は、図５のデータベース局の一部を形成する記憶装置の内容を図解する。図７は、図１の実施形態において、衛星によって生成されるビームを概要的に図解する。図８は、地球の周りの軌道において、図１の一部を形成する衛星の配置を概要的に図解する。図９は、本発明の第１実施形態において、図２の送受器の構成要素間における信号の流れを示すブロック図である。図１０は、第１実施形態において、図１の構成要素間における暗号化データおよび信号の流れを示す概要的なブロック図である。図１１は、第１実施形態において、図９の送受器の制御および暗号化構成要素によって実行される処理を概要的に示す流れ図である。図１２は、第１実施形態において、図３の地球局の動作の処理を概要的に示す流れ図である。図１３は、第１実施形態において、図４の中央データベース局の動作の処理を概要的に示す流れ図である。図１４は、第１実施形態において、図９の送受器内に収容された加入者情報モジュール（ＳＩＭ）の動作の処理を概要的に示す流れ図である。図１５は、本発明の第４実施形態で提供された安全性のステージを概要的に図解する流れ図である。図１６は、図９の第１送受器端末による暗号化キーの形成のステージを示す図解的な図である。図１７は、そのような第２送受器における暗号化キーの形成の処理を示す対応する図解的な図である。図１８および図１９は、本発明の第３実施形態において、図１３および図１４の流れ図の動作を変更する流れ図である。図２１は、本発明の第４実施形態に従った図９の送受器内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。図２２は、第４実施形態のデータベース局内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。図２３は、第４実施形態の地球局内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。（図１１の組み込み部である）図２４は、第４実施形態に従った送受器の動作を概要的に示す流れ図である。（図１２の組み込み部である）図２５は、第４実施形態に従った地球局の動作の処理を概要的に示す流れ図である。（図１３の組み込み部

である）図２６は、第４実施形態に従ったデータベース局の動作を概要的に示す流れ図である。（図１４の組み込み部である）図２７は、第４実施形態に従った加入者情報モジュールの動作を概要的に示す流れ図である。図２８は、本発明の実施形態が、３以上の使用者端末を伴う電話会議のために、どのように使用され得るのかを図解する。

【００２１】図１を参照すると、この実施形態に従った衛星通信ネットワークは、移動使用者端末装置２ａ，２ｂと、軌道周回中継衛星４ａ，４ｂ，４ｃと、衛星地球局ノード６ａ，６ｂ，６ｃと、衛星システムゲートウエー局８ａ，８ｂと、公衆交換遠距離通信ネットワーク１０ａ，１０ｂと、固定遠距離通信端末装置１２ａ，１２ｂとを具備している。

【００２２】衛星システムゲートウエー８ａ，８ｂ，８ｃと地球局ノード６ａ，６ｂ，６ｃとの相互結合、および、ノード６ａ，６ｂ，６ｃ同士の相互結合は、チャネル１４ａ，１４ｂ，１４ｃを具備する専用地上ベースネットワークである。衛星４と地球局６と線１４とは、衛星通信ネットワークの基本的構造を構成する。この衛星通信ネットワークは、移動端末２との通信のためのものであり、かつ、ゲートウエー局８を通してアクセス可能である。端末位置データベース局１５は、（例えば、専用ネットワークのチャネル１４内部の）信号送信リンク６０を介して、ゲートウエー局および地球局６に接続されている。

【００２３】ＰＳＴＮ１０ａ，１０ｂは、典型的には、局所交換機１６ａ，１６ｂと国際スイッチングセンター２０ａ，２０ｂとを具備する。固定端末装置１２ａ，１２ｂは、局所ループ１８ａ，１８ｂを介して、局所交換機１６ａ，１６ｂに接続されている。国際スイッチングセンター２０ａ，２０ｂは、トランスナショナルリンク２１（例えば、衛星リンクまたは海底光ファイバケーブルリンク）を介して、互いに接続可能である。ＰＳＴＮ１０ａ，１０ｂおよび固定端末装置１２ａ，１２ｂ（例えば、電話器）は、よく知られており、かつ、今日では常に全世界で利用可能である。

【００２４】各移動端末装置は、（この実施形態において、）全２重チャネルを介して、衛星４と通信している。この全２重チャネルは、ダウンリンクチャネルとアップリンクチャネルとを具備している。このダウンリンクチャネルとアップリンクチャネルは、例えば（その各場合において）呼の開始時に割り当てられた特定周波数上のＴＤＭＡタイムスロットであり、このことは、英国特許出願第２２８８９１３号および英国特許出願第２２９３７２５号に開示されている。この実施形態の衛星４は、非静止衛星であり、故に、周期的に、ある衛星４から他の衛星４への移管がある。

【００２５】●移動端末２

図２を参照すると、図１の移動端末装置が示されている。１つの適した形態は、示されるような送受器である。送受器２ａ，２ｂ等の詳細は、説明されておらず、かつ、ＧＳＭシステムでの使用のために現在利用可能な送受器に類似している。この送受器は、衛星通信に適した従来のマイクロフォン３６，ラウドスピーカ３４，バッテリ４０，キーパッドコンポーネント３８，無線周波数（ＲＦ）インターフェース３２，アンテナ３１と共に、デジタルコーダ／デコーダ３０を具備している。好ましくは、ディスプレイ３９（例えば、液晶ディスプレイ）も設けられる。使用者情報を記憶するスマートカード（ＳＩＭ）３５を収納する「スマートカード」リーダー３３も設けられる。

【００２６】コーダ／デコーダ（コーデック）３０は、チャネルコーダと共に、低ビットレートコーダを具備する。低ビットレートコーダは、約３．６キロビット／秒で音声ビットストリームを生成する。チャネルコーダは、符号化されたビットストリームを、４．８キロビット／秒のレートで生成するために、誤差訂正符号化に適用する。低ビットレートコーダは、例えば、マルチパルス予測コーダ（ＭＰＬＰＣ）または符号駆動型線形予測コーダ（ＣＥＬＰ）または残余駆動型線形予測コーダ（ＲＥＬＰ）のような線形予測コーダである。この他にも、低ビットレートコーダは、（副帯域符号化のような）いくつかの形式の波形符号化を使用する。

【００２７】適用された誤差保護符号化は、ブロックコードまたはＢＣＨコードまたはリードソロモン（Reed-Solomon）コードまたはターボコードまたは重畳コードを使用する。コーデック３０は、同様に、対応するチャネルデコーダおよび音声デコーダを具備する。このチャネルデコーダは、ビタービ（Viterbi）またはソフト決定符号化を使用する。制御回路３７も設けられる。制御回路３７は、実際には、適切にプログラムされたマイクロプロセッサ、または、マイクロコントローラ、または、デジタルシグナルプロセッサ（ＤＳＰ）チップからなるコーダ３０と組み合わされる。

【００２８】ＳＩＭ３５は、好ましくは、ＧＳＭ勧告02.17「加入者識別モジュール」および11.11を満たしており、好ましくは、工業規格「スマートカード」として実行される。故に、ＳＩＭ３５およびリーダー３３は、好ましくは、国際標準ISO 7810, 7811, 7816に説明されるとおりである。これらの国際標準およびGSM 02.17, 11.11は、全て、参照によって本明細書に組み込まれる。具体的に、ＳＩＭ３５は、プロセッサ３５ａおよび固定記憶装置３５ｂを具備している。プロセッサ３５ａは、以下に非常により詳細に説明されるようないくつかの暗号化機能を実行するように用意されている。

【００２９】●地球局ノード６

地球局ノード６は、衛星との通信のために用意されている。各地球局ノード６は、図３に示されるように、従来の衛星地球局２２を具備する。衛星地球局２２は、少な

くとも１つの移動している衛星４を追跡するように用意された少なくとも１つの衛星追跡アンテナ２４と、アンテナ２４へ信号を供給するＲＦ電力増幅器２６ａと、アンテナ２４から信号を受信するＲＦ電力増幅器２６ｂと、衛星天体位置表データ記憶し、かつ、アンテナ２４のステアリングを制御し、かつ、（アンテナ２４を介して衛星４に信号送信することによって）要求される衛星４の全ての制御を達成する制御ユニット２８とからなる。

【００３０】地球局ノード６は、移動衛星スイッチングセンター４２をさらに具備する。移動衛星スイッチングセンター４２は、専用ネットワークの一部を形成する幹線リンク１４に接続されたネットワークスイッチ４４を具備する。マルチプレクサ４６は、スイッチ４４からのスイッチされた呼を受信するように、かつ、スイッチされた呼を、低ビットレート音声コーデック５０を介して増幅器２６へ供給するためのコンポジット信号に、マルチプレクスするように用意されている。地球局ノード６は、また、ノード６が通信している衛星４によって処理されるエリア内の各移動端末装置２ａの詳細を記憶する局所記憶装置４８を具備している。

【００３１】●ゲートウエー８

図４を参照すると、ゲートウエー局８ａ，８ｂは、この実施形態において、ＧＳＭシステムのようなデジタル移動セルラー無線システムで使用されるタイプの商業的に利用可能な移動スイッチングセンター（ＭＳＣ）を具備する。ゲートウエー局８ａ，８ｂは、この他に、ＰＳＴＮ１０ａ，１０ｂのうちの１つを形成する国際または他の電話交換局の一部を具備する。ＰＳＴＮ１０ａ，１０ｂは、ソフトウェア制御の下で、ネットワーク１０を衛星システム幹線リンク１４と相互結合するように動作する。

【００３２】ゲートウエー局８は、ＰＳＴＮ１０からの入力ＰＳＴＮ線を、制御ユニット７２の制御の下で、１または２以上の地球局ノード６と接続された専用サービス線１４と相互結合するように用意されたスイッチ７０を具備する。制御ユニット７２は、信号送信ユニット７４を介してデータベース局１５に接続されたデータチャネル６０と通信でき、かつ、（例えば、パケットまたはＡＴＭセルのような）ある適したフォーマットでデータメッセージを生成するように用意されている。

【００３３】ゲートウエー局８には、ゲートウエー局８が基地ゲートウエー局である移動端末２に関して、その請求書とサービスと他の情報とを記憶する記憶装置７６も設けられている。データは、衛星ネットワークを構成するＰＳＴＮ１０または地球局ノード６から、信号送信ユニット７４またはスイッチ７０を介して受信された後、制御ユニット７２によって記憶装置７６に書き込まれる。この記憶装置は、地上のＧＳＭネットワークのビジター位置レジスタ（ＶＬＲ）の方法で動作する。故に、商業的に利用可能なＶＬＲは、記憶装置７６で使用されてもよい。

【００３４】衛星システム幹線１４は、この実施形態において、信号減衰および遅延に対する許容可能な最小基準を満たす高品質賃貸線を具備する。この実施形態では、全ての線１４は、地上のリンクを具備する。幹線リンク１４は、好ましくは、専用線である。そのため、線１４は、ネットワーク１０への物理的なチャネルの個々の組を形成する。しかしながら、ネットワーク１０を通した仮想回路の使用は、除かれない。

【００３５】●データベース局１５

図５を参照すると、データベース局１５は、デジタルデータ記憶装置５４と信号送信回路５６とプロセッサ５８と信号送信リンク６０とを具備する。プロセッサ５８は、信号送信回路５６および記憶装置５４と相互結合されている。信号送信リンク６０は、データベース局１５を、衛星システムネットワークを構成するゲートウエー局８および地球局６と相互結合しており、信号送信またはデータメッセージ通信のためのものである。

【００３６】記憶装置５４は、全ての加入者端末装置２について、識別子（例えば、国際移動加入者識別子すなわちＩＭＳＩ）を示す記録を含む。この識別子は、端末２の現在の状態（以下により詳細に示されるような「ローカル」または「グローバル」のどちらであるか）と、移動端末２の地理的位置（座標形状で示されてもよいし、または、移動端末２が存在するエリアを識別するコードとして示されてもよい）と、（請求書および他のデータが一ヵ所に集められる得るように）装置が登録された「基地」ゲートウエー局８と、装置２が衛星４を介して通信している現在有効な地球局ノード６とである。記憶装置の内容は、図６に示されている。さらに、この実施形態では、記憶装置は、各使用者について、特有かつ個別の暗号化キーＫｉを含む。この暗号化キーＫｉは以下に説明されるように使用され得る。

【００３７】信号送信ユニット５６およびプロセッサ５８は、ゲートウエー８またはノード６から、パケットスイッチされた接続である信号送信リンク６０を介して、質問データメッセージを受信するように用意されている。このデータメッセージは、移動端末２のうちの１つを識別するデータ（例えば、装置２の電話番号）を具備する。そして、プロセッサ５８は、端末２の状態および有効地球局ノード６のために記憶装置５４を探索するように、かつ、端末２の状態および有効地球局ノード６をデータ線６０を介して返答メッセージで送信するように用意されている。故に、この実施形態では、データベース局１５は、ＧＳＭシステムの基地位置レジスタ（ＨＬＲ）とＧＳＭシステムの識別検証センター（ＡｕＣ）との両方の機能を満足するように動作し、かつ、商業的に利用可能なＧＳＭ製造物に基づく。

【００３８】●衛星４

衛星４ａ，４ｂは、一般的に、（既知のヒューズＨＳ６０１型のような）従来の通信衛星を含み、かつ、英国特許出願第２２８８９１３号に開示されるような特徴を具備する。各衛星４は、衛星の下のフットプリントをカバーするビームのアレイを生成するように用意されている。各ビームは、英国特許出願第２２９３７２５号で説明されるような、かつ、図７に図解されるような多数の異なる周波数チャネルおよびタイムスロットを具備する。

【００３９】衛星４は、地球の十分なエリアをカバーするのに（好ましくは、完全な連続した全世界の範囲を与えるのに）十分な数および適した軌道の衛星群内に用意されている。例えば、１０または１１以上の衛星が、図８に示されるように、２つの相互に直交した（例えば、高度１０，５００キロメートルの）中間円形軌道内に、設けられている。しかしながら、例えば、イリジウムシステムに関する欧州特許出願第０３６５８８５号または他の刊行物に示されるように、より多い数のより低い衛星が使用されてもよい。

【００４０】●登録および位置

ある実施形態において、顧客移動端末装置２は、２つの異なる状態のうちの１つで登録されている。１つは「ローカル」であり、この場合、移動端末装置は、１つのローカルエリア、または、衛星システムネットワークの一部を通して通信することだけを許可される。もう１つは「グローバル」であり、これは、装置に対して、衛星システムネットワークの全ての部分を通して通信する資格を与える。各装置２の状態（即ち「ローカル」または「グローバル」）は、図６に示されるように、データベース局１５の記憶装置５４内において、関連する装置２のために保持された記録内に記憶される。

【００４１】端末２が出力呼のために利用される場合、および／または、装置２がオンに切り替えられる場合、および／または、周期的に装置２がオンに切り替えられる間の各場合において、移動端末装置２は、セルラー地上通信の技術ではよく知られた種類の自動登録処理を実行する。従来からそうであるように、登録処理は、（例えば、共通の呼出しまたは信号送信周波数上でその電話番号を送信することによって）移動端末２を識別する信号の同報通信の形式をとる。

【００４２】送信された信号は、１または２以上の衛星４によってピックアップされる。通常の環境の下では、信号は、複数の衛星４によってピックアップされる。そして、受信された信号強度および／または到達時間は、移動装置２の識別子および（信号を受信した）衛星４の識別子と共に、衛星４が通信中の（１または複数の）地球局ノード６および信号送信リンク６０を介して、データベース局１５に送信される。

【００４３】そして、データベース局１５のプロセッサ５８は、例えば、差異のある到達時間に基づいて、移動端末装置２の地上の位置を計算し、この位置は、データベース５４内に記憶される。移動端末装置２との通信に最も適した地球局ノード６（即ち、「有効な」局）の識別子も記憶される。この地球局ノード６は、プロセッサ５８が、端末２の記憶された位置を各々の地球局ノード６の予め記憶された位置と比較し、かつ、最も近いものを選択することによって、典型的に発見される。しかしながら、衛星４を介して受信された信号の強度、または、（ネットワークの密集のような）他の要因もまた、あるいは、代わりに、考慮されてもよい。このネットワークの密集は、境界線の場合に、移動端末装置２に地理的に最も近いわけではないノード地球局の選択をもたらす。そして、割り当てられた有効な地球局ノード６の識別子は、同様に、（記憶装置５４において、）端末装置に対する記録内に記憶される。

【００４４】●呼の設定およびルーチング

移動端末装置２への、および、移動端末装置２からの呼のルーチングの処理は、英国特許公開２２９５２９６号公報およびＰＣＴ／ＧＢ９５／０１０８７に完全に記載されている。この両方は、参照によって、本明細書に完全に組み込まれる。簡単に説明すると、そのエリア外のローカル使用者に対して、使用者へまたは使用者から配置された呼は、データベース局に参照される。データベース局は、使用者がそのエリア外にいることを判断し、その後、呼を処理しない。

【００４５】そのエリア内にいるローカル使用者に対して、上記参照の英国および国際出願に記載された好ましい実施形態では、移動使用者および（ＰＳＴＮのうちの１つに接続された）従来の地上の使用者へまたはこれらの使用者からの呼は、有効な地球局６と地上ネットワークと国際公衆交換電話ネットワーク（ＰＳＴＮ）とを介して、最も近いゲートウエーから地上の使用者へ、衛星リンクを通して設定される。グローバル使用者に対して、呼は、衛星および有効な地球局を介して、そして、地上のネットワークを介して、地上の使用者に最も近いゲートウエー局８へルーチングされる。

【００４６】移動使用者に割り当てられたダイヤル番号は、衛星サービスネットワークに対応するコードによって続かれる「国際」局番を有する。この他にも、上記ダイヤル番号は、衛星サービスに割り当てられた地域コードによって続かれる国局番を有することができる。ある移動使用者と他の移動使用者との間の呼は、第１移動使用者の有効な地球局ノードへ下がる第１衛星リンクと、第２移動使用者（これは、必ずしもそうである必要はないが、第１の移動使用者と同じであってもよい）の有効な地球局への地上ネットワークと、第２移動使用者への第２衛星リンクとを介して（これは、必ずしもそうである必要はないが、同じ衛星を介してもよい）、信号を送ることによって実行される。

【００４７】●第１実施形態

図９は、図２の移動端末の構成要素を通した信号フローを、より詳細に示す。空中線３１から受信された信号は、ＲＦモデム３２によって、ＲＦ復調され、かつ、プロセッサ回路３７へ供給される。プロセッサ回路３７は、暗号化モード時において、受信されたデータを（例えば、ＳＩＭ３５から供給される解読キーに従ったＡ５アリゴリズムを使用して）解読するように用意されている。解読キーは、Ka,bとして参照される。

【００４８】そして、解読されたビットストリームは、誤差訂正デコーディングを実行するチャネルコーデック３０ｂへ送られる。そして、誤差訂正された音声信号は、低ビットレートコーデック３０ａへ供給される。低ビットレートコーデック３０ａは、デジタル／アナログ変換器を具備する。デジタル／アナログ変換器の出力は、ラウドスピーカ３４へ供給される。

【００４９】マイクロフォン３６からの音声は、低ビットレートコーデック３０ａへ供給される。低ビットレートコーデック３０ａは、アナログ／デジタル変換器を具備する。結果として生じる低ビットレート音声信号は、誤差保護を含むために、チャネルコーデック３０ｂによって符号化される。そして、誤差保護されたビットストリームは、暗号化モードの場合、制御回路３７によって暗号化される。そして、暗号化されたビットストリームは、空中線３１からの送信のために、ＲＦモデム３２に供給される。

【００５０】図１０～図１２を参照すると、通信の暗号化されたモードの設定処理は、ここで、より詳細に説明されている。２つの使用者端末２ａ，２ｂの間での通信セッションの間、１または両方の端末の使用者は、暗号化された形式での会話を続けることを選択する。従って、図１１を参照すると、ステップ１００２において、実施するパーティは、キーボード３８からの一連のキーの打ち込みを入力するか、または、安全性を引き起こすための指示としてプロセッサ３７によって認識される特殊キーを操作する。従って、プロセッサ３７は、ステップ１００２において、帯域内または関連する制御チャネル上での暗号化を引き起こすための信号を送信する。

【００５１】図１２を参照すると、地球局６では、ステップ１１０２において、プライバシー要求信号が受信される。ステップ１１０４において、その信号が、端末２ａ，２ｂの識別子を示す識別子コードと共に、中央データベース局１５に送られ、かつ、第２使用者端末２ｂに送られる。第２使用者端末２ｂでは、プライバシー信号の受信が、図１１のステップ１００２において発生する。

【００５２】図１３を参照すると、中央データベース局では、プライバシー信号がステップ１２０２において受信される。ステップ１２０４において、データベース局１５のコントローラ５８は、メモリ５４にアクセスし、かつ、第１移動端末２ａに対して記憶された個々の暗号化キーKaと、第２移動端末２ｂに対して記憶されたキーKbとを読み出す。ステップ１２０６において、コントローラ５８は、疑似ランダム数（ＲＡＮＤ）を生成する。この実施形態では、キーKa，Kbは、それぞれ、１２８ビットの２進数であり、かつ、ランダム数ＲＡＮＤは、他の１２８ビットの２進数である。

【００５３】ステップ１２０８において、コントローラ５８は、第１部分キーKaおよび第２部分キーKpbを計算する。第１部分キーの計算は、図１６に図解されている。この計算は、１２８ビットの数の生成を具備する。この１２８ビットの各ビットは、第２端末キーKaの対応する位置のビットとランダム数ＲＡＮＤとの排他的論理和関数を具備する。故に、第２部分キーは、以下のように与えられる。

Kpa＝Ka＋ＲＡＮＤ

（ここで、＋は２進の加算操作を示す）

【００５４】第２部分キーKpbは、正確に同じ方法で、即ち、図１６に示されるように、第１端末キーKbとランダム数ＲＡＮＤとの間でビット単位の排他的論理和処理を実行することによって、計算される。図１３のステップ１２１０において、中央データベース局１５は、信号送信ネットワーク６０と個々の地球局６ｂ，６ａと衛星４ｂ，４ａとを介して、第１部分キー（Kpa）を第１端末２ａに送信し、かつ、第２部分キー（Kpb）を第１端末２ｂに送信する。

【００５５】このステージでは、各個別の端末キーは、ランダム数ＲＡＮＤとの２進加算操作によって「撹乱」されている。２つの未知数（ランダム数ＲＡＮＤと端末キー）が存在するので、部分キーのうちの１つを監視している許可されていない盗聴者は、その部分キーから端末キーを知ることができない。両方の部分キーを監視している許可されていない盗聴者でさえも、（３つの未知数を引き出すための）たった２つのデータしか有しないので、ランダム数と端末キーのうちの１つとのどちらも引き出すことができない。引き出され得る最良のものは２つの端末キー間の差であり、それは意味がない。

【００５６】ここで、図１２を参照すると、ステップ１１０６において、各地球局は、部分キーを受信し、かつ、ステップ１１０８において、その部分キーを移動端末へ送る。図１１を参照すると、ステップ１００４において、各々の移動端末（２ａ，２ｂ）は、対応する部分キー（Kpa，Kpb）を受信する。ステップ１００６において、部分キーは、カードリーダー３３を介して、ＳＩＭ３５へ送信される。

【００５７】図１４を参照すると、ステップ１３０２において、ＳＩＭは、部分キーを受信する。そして、ステップ１３０４において、ＳＩＭは、メモリ３５ｂ内から端末キーを読む。ステップ１３０６において、ＳＩＭプロセッサ３５ａは、新しい１２８ビットの２進数を生成するために、部分キーKpaから、記憶されている端末キ

ーKaを比較することによって、２進のランダム数ＲＡＮＤを復元する。この比較ステップは、KpaとKaとの排他的論理和演算によって実行される。故に、ＳＩＭプロセッサは、

KR＝Kpa

＝Ka＋（ＲＡＮＤ）－Ka

＝（ＲＡＮＤ）

であるコードKRを計算する。ステップ１３０８において、ＳＩＭ３５は、KR＝（ＲＡＮＤ）を、カードリーダーデバイス３３を介して、端末プロセッサ３７へ供給する。コードKRは、送信されるべきデータに対する暗号化キーとして使用される。

【００５８】同様に、第２端末２ｂでは、端末のＳＩＭ内において、記憶されている値Ｋｂが第２部分キーKpbから減算されることによって、即ち、

KR＝Kpb－Kb

＝Ｋｂ＋（ＲＡＮＤ）－Kb

＝（ＲＡＮＤ）

によって、KR＝（ＲＡＮＤ）の値が計算される。故に、各端末２ａ，２ｂは、同一の暗号化キーKR＝（ＲＡＮＤ）を計算する。

【００５９】図１１に戻って参照すると、ステップ１００８において、端末プロセッサ３７は、暗号化キーKRを受信する。そして、ステップ１０１０において、端末３７は、暗号化モードに切り替わる。その後、ステップ１０１２では、プロセッサ３７は、ＲＦ変調および送信の前に、コーデック３０からのビットストリームを暗号化するように機能し、かつ、ＲＦモデム３２からの対応するビットストリームをコーデック３０へ（キーKRを使用して）供給する前に、そのビットストリームを解読するように機能する。暗号化キーKRそれ自身が秘密なので、暗号化アリゴリズムは、いかなる適したアリゴリズムでもよく、かつ、広く知られていてもよい。暗号化アリゴリズムは、好都合には、ＧＳＭ送受器で使用されるＡ５アリゴリズムであり、かつ、上記参照されるＧＳＭ勧告に記載されている。

【００６０】故に、要約すると、図１０に示されるように、この実施形態において、各端末２は、関連する特有の端末キーを有する。この端末キーは、端末内に収容されたＳＩＭ３５内に、または、中央データベース局１５内に、記憶されている。使用される暗号化キーKRは、遠く離れたデータベース局１５で生成されたランダム数（ＲＡＮＤ）の関数である。このデータベース局１５は、ランダム数（ＲＡＮＤ）を、マスクされた形式で（即ち、部分キーKpa，Kpbで）、端末２ａ，２ｂへ分配する。

【００６１】端末キーをマスクされた形式で送信することは、盗聴者が各端末キーへアクセスすることを防止する。各セッション操作におけるマスクを変化させることにより、即ち、疑似ランダム数（ＲＡＮＤ）の連続して

変化するシーケンスを生成することにより、盗聴者は、終始、マスク関数を知ることができない。端末キーは端末それ自身からさえもマスクされているので、各端末またはＳＩＭもまた、他の端末キーを解くことはできない。

【００６２】●第２実施形態

第２実施形態では、中央データベースにおける許可されていない干渉に対する機会を減少することによって、安全性はさらに改良される。第２実施形態は、図１５に示されるように、図１３のステップ１２０４～１２１０が実行される代わりに、ステップ１４０４～１４２０が実行されることを除くと、ほぼ第１実施形態と同様に動作する。

【００６３】従って、ステップ１２０２の後に、プロセッサ５８は、最初に、ステップ１４０４において、第１端末キーKaにアクセスし、そして、（ステップ１２０６に関して記載されたように）ステップ１４０６において、ランダムな数を計算し、そして、（ステップ１２０８に関して記載されたように）ステップ１４０８において、第１部分キーKpaを計算し、そして、（ステップ１２１０に関して記載されたように）ステップ１４１０において、第１部分キーを送る。

【００６４】これらの処理の後、KaおよびKpaの全ての局所的に記憶されたコピーが消去される。そして、ステップ１４１４において、プロセッサ５８は、第２端末キーＫｂにアクセスし、第２部分キーKpbを計算し（ステップ１４１６）、第２部分キーを送り（ステップ１４１８）、第２部分キーおよび第２端末キーを消去する（ステップ１４２０）。故に、この実施形態では、２つの部分キーおよび端末キーへのアクセスは、時間において分離されており、データベース局１５の盗聴および不正利用を減少する。

【００６５】２つの部分キーおよび／または端末キーへのアクセスは、他の方法（例えば、２つの端末キーを物理的に分離された装置へ送り、そして、端末キーと組み合わせるための各々の装置へランダム数を送る方法）で分離され得る。同じランダム数を２つの異なる装置へ送るよりもむしろ、追加の安全性のために、２つの同一の同期したランダム数生成器が、２つの異なる位置に設けられる。２つの端末キーは、その２つの異なる位置に送られる。故に、２つの端末キーおよび／または部分キーへのアクセスは、時間においても、または、時間における代わりに、物理的に分離される。

【００６６】●第３実施形態

この実施形態では、送信に対する各々の部分キーKpaを暗号化することによって、安全性は、さらに増加する。共通の暗号を使用することは可能であるが、共通の暗号へのアクセスを用いる盗聴者（例えば、プライバシーサービスの許可された他の使用者）が暗号を解読できるので、これは望ましくない。同様に、ＧＳＭシステムにお

いて既知の型の空中インターフェース暗号は、ネットワークの固定部分における傍受に対して開かれているので、この暗号を使用しないことが好ましい。

【００６７】従って、この実施形態では、ＳＩＭ３５は、（好都合には、ＧＳＭシステムで使用されるＡ５アリゴリズムである）解読アリゴリズムを記憶し、かつ、データベース局１５は、対応する暗号化アリゴリズムを実行するように用意されている。図１８を参照すると、この実施形態において、第１実施形態の図１３の処理は、ステップ１２０８とステップ１２１０との間のステップ１２０９の包含によって、変更されている。ステップ１２０９では、各部分キーは、部分キーが送られた端末の端末キーを使用して暗号化され、かつ、暗号化形式で送信される。

【００６８】図１９を参照すると、この実施形態において、各端末では、ＳＩＭプロセッサ３５ａは、ステップ１３０４とステップ１３０６との間の追加のステップ１３０５を実行する。ステップ１３０５において、受信された部分キーは、暗号化キーを計算する前に、端末キーを使用して解読される。故に、この実施形態において、送信された部分キーを暗号化することによって、追加の安全性が行われる。好都合には、暗号化は、目的端末の端末キーを使用する。そこで、暗号化データをさらに記憶する必要性を避けることができる。しかしながら、明白なことには、他の形式の暗号化が可能であり、特に、らに洗練された暗号化アリゴリズム（追加のランダム数も送られるアリゴリズム）が可能である。

【００６９】●第４実施形態

この実施形態では、第１実施形態の原理が、（ＧＳＭ互換ネットワークに見られ、かつ、上記ＧＳＭ勧告内に明確にされている）空中インターフェース暗号化および識別検証システムと組み合わせて利用される。図１５を参照すると、安全性の特徴は、以下の順番で適用される。

識別検証（ステップ２００２）

空中インターフェース暗号化（ステップ２００４）

端末相互暗号化（ステップ２００６）

【００７０】最初の２つのステップは、現存するＧＳＭネットワークにおける通りであり、、かつ、３番目は、第１実施形態に関して上述された通りである。ここで、処理は、さらに詳細に説明される。図２１を参照すると、送受器プロセッサ３７およびＳＩＭ３５によって実行される機能は、個々の機能ブロックとして説明されている。各機能ブロックは、当然のことながら、個々のマイクロプロセッサまたはデジタルシグナルプロセッサ（ＤＳＰ）装置によって実行され得る。しかし、この実施形態では、実際には、１つのそのようなプロセッサ装置が送受器内に存在し、１つのそのようなプロセッサ装置がＳＡＮ３５内に存在するだけである。

【００７１】図２１を参照すると、アンテナ３１から受信され、かつ、ＲＦモデム３２によって復調された信号は、第１暗号化／解読ステージ３７２と第２暗号化／解読ステージ３７４とを通って送られる。第１暗号化／解読ステージ３７２は、空中インターフェース暗号化キーKcに従ってＧＳＭから知られるＡＳアリゴリズムを適用するように用意されている。第２暗号化／解読ステージ３７４は、端末相互暗号化キーKa,bに従って解読する第２解読アリゴリズムを適用するように用意されている。第２解読アリゴリズムは、好都合には、再び、ＧＳＭシステムで使用され、かつ、上記勧告に記載されるＡ５アリゴリズムである。その後、解読されたビットストリームは、コーデック３０に供給される。同様に、コーデック３０からの音声ビットストリームは、２つの暗号化／解読ステージ３７２，３７４を逆の順番で通って送られる。簡単化のために、その信号経路は、図２１から省略されている。

【００７２】ＳＩＭ３５内には、端末キー記憶レジスタ３５２が配置されている。端末キー記憶レジスタ３５２は、端末に対する端末キーKa（この場合、端末２ａに対するKa）を記憶する。端末キー記憶レジスタ３５２は、端末キーKaを供給するために、署名計算ステージ３５４に接続されている。署名計算ステージ３５４は、Ａ３アリゴリズムに従って端末を識別検証するために使用される「署名された応答」数（ＳＲＥＳ）を計算するように用意されている。Ａ３アリゴリズムは、上述されたＧＳＭ勧告に記載されており、かつ、ＧＳＭシステムで使用される。応答計算ステージ３５４は、また、カードリーダー装置３３を介して、ＲＦモデム３２からの暗号化されていないビットストリーム出力から、ランダム数（ＲＡＮＤ１）を受信するために、接続されている。

【００７３】端末キーレジスタ３５２は、また、端末キーKaを供給するために、第１キー生成ステージ３５６に接続されている。第１キー生成ステージ３５６は、また、ランダム数（ＲＡＮＤ１）を受信し、かつ、Ａ８アリゴリズムに従ってランダム数（ＲＡＮＤ１）から空中インターフェース暗号化キーKcを計算するように用意されている。Ａ８アリゴリズムは、上記ＧＳＭ勧告に記載されており、かつ、ＧＳＭシステムで使用される。このようにして計算されたキーは、カードリーダー装置３３を介して、端末プロセッサ３７の第１（空中インターフェース）暗号化／解読ステージ３７２へ供給される。

【００７４】端末キーレジスタ３５２は、また、端末キーを供給するために、第２キー生成ステージ３５８に接続されている。第２キー生成ステージ３５８は、端末キーKaと部分キーKpaとを利用する（第１実施形態で説明されたような排他的論理和機能による）端末相互暗号化のための暗号化キーKRを生成するように用意されている。第２キー生成ステージ３５８は、端末プロセッサ３７の第１（空中インターフェース）暗号化／解読ステージ３７２の解読された出力から（カードリーダー装置３３を介して）受信するために、接続されている。この

ようにして計算された端末相互暗号化キーは、端末プロセッサ３７の第２（端末相互）暗号化／解読ステージ３７４へ供給される。

【００７５】図２２を参照すると、中央データベース局１５は、この実施形態において、ランダム数生成器５８２と記憶装置５４とキー生成ステージ５８４と署名計算ステージ５８６とを具備する。ランダム数生成器５８２は、使用の度に、無作為の順番で新たな２進１２８ビット数（ＲＡＮＤ１）を生成するように用意されている。記憶装置５４は、端末キーＫｉを記憶する。キー生成ステージ５８４は、記憶装置５４からの端末キーとランダム数（ＲＡＮＤ１）とを受信し、かつ、Ａ８アリゴリズムに従って、この端末キーおよびランダム数（ＲＡＮＤ１）から、空中インターフェース暗号化キーＫｃを計算するために接続されている。Ａ８アリゴリズムは、ＧＳＭ勧告に記載されており、かつ、ＧＳＭシステムで使用される。署名計算ステージ５８６は、同様に、端末キーとランダム数（ＲＡＮＤ１）とを受信するために接続されており、Ａ３アリゴリズムに従って、署名された応答数（ＳＲＥＳ）を計算するように用意されている。Ａ３アリゴリズムは、上述したＧＳＭ勧告に記載されており、かつ、ＧＳＭシステムで使用される。

【００７６】ランダム数生成ステージ５８２と署名応答生成ステージ５８６とキー生成ステージ５８４との出力は、地球局６への送信のための信号送信回路５６に接続されている。図２３を参照すると、各地球局６は、（データベース４８内に、）３連レジスタ４８２を具備する。３連レジスタ４８２は、３連の予め決められた数（例えば５）を記憶するように用意されている。上記３連は、それぞれ、信号送信リンク６０を介してデータベース局１５から供給されたランダム数と対応ＳＲＥＳと対応空中インターフェース暗号化キーＫｃとを具備する。

【００７７】移動端末２が地球局６を登録する度に、地球局は、３連の予め決められた数の（中央データベース局１５からの）供給を要求する。従って、中央データベース局１５は、３連の予め決められた数を生成し、かつ、それらの数を、信号送信リンク６０を介して、レジスタ４８２での記憶のために送信する。比較器２８２もまた、地球局６内に設けられている。比較器２８２は、３連レジスタ４８２に結合され、かつ、地球局６の空中インターフェース構成要素２４，２６に結合されている。比較器２８２は、移動端末２から受信される署名された応答（ＳＲＥＳ）数を、レジスタ４８２に記憶された署名された応答と比較し、かつ、２つの数の間の通信（または、通信がないこと）を示すように用意されている。もし、２つの数が一致しないならば、使用者は識別検証されず、かつ、サービスは制御ユニット２８によって中止される。

【００７８】最後に、地球局６は、空中インターフェース暗号化ステージ２８４を具備する。空中インターフェース暗号化ステージ２８４は、（ＧＳＭから知られる）ＡＳアリゴリズムに従って、３連レジスタ４８２から供給される空中インターフェース暗号化キーＫｃを使用して、暗号化および解読するために用意されている。暗号化の方向では、空中インターフェース暗号化／解読ステージ２８４は、コーデック５０（図３）からの入力を受信し、かつ、その出力を空中インターフェース構成要素２４，２６に発する。ところが、解読の方向では、暗号化／解読ステージ２８４は、空中インターフェース構成要素２４，２６からその入力を受信し、かつ、その出力をコーデック５０へ発する。

【００７９】この実施形態の動作は、ここで、図２４～図２７を参照して、より詳細に説明される。図２４～図２７において、（さらに詳細には説明されない）図１１～図１４の処理のステップが組み込まれる。図１１にあるとおり、プライバシーに対する要求が、パーティのうちの１人によって開始され、かつ、プライバシー要求信号は、端末２ａから送信される。地球局６ａでのプライバシー信号の受信（ステップ１１０２）、および、データベース局１５へのプライバシー信号の送信（ステップ１１０４）に続いて、図１３を参照すると、ステップ１２０２，１２０４は、２つの端末の端末キーを生じるために、実行される。

【００８０】そして、ステップ１２０５において、端末相互暗号化を使用することを両方の加入者が識別検証されるか否かを判断するために、判断が実行される。もし、両方の加入者が識別検証されるならば、図１３のステップ１２０６～１２１０が実行される。次に、または、もし、両方の加入者が識別検証されないならば、データベース局１５は、ステップ１２１２に進む。ステップ１２１２において、データベース局１５は、地球局６ａ，６ｂに信号を送信する。地球局６ａ，６ｂは、２つの端末２ａ，２ｂが、端末識別検証チェックを実行し、かつ、空中インターフェース暗号化を開始するように指示するように、２つの端末２ａ，２ｂを処理する。

【００８１】図２５に戻って参照すると、各地球局６は、指示信号および部分キーの受信時（ステップ１１１０）に、識別検証質問メッセージを送る（ステップ１１１２）。識別検証質問メッセージは、３連レジスタ４８２から得られる次のランダム数ＲＡＮＤ１を含む。さらに、ＧＳＭシステムにおけるように、キー番号は、さらなる確認のために送信される。図２４に戻って参照すると、識別検証要求メッセージの受信時（ステップ１０１４）に、ランダム数（ＲＡＮＤ１）は引き出され、かつ、ＳＩＭ３５に送られる（ステップ１０１６）。

【００８２】図２７を参照すると、ＳＩＭ３５において、ランダム数ＲＡＮＤ１の受信時（ステップ１３１０）に、ＳＩＭプロセッサ３５ａは、端末キーＫａを捜し（ステップ１３１２）、かつ、署名された応答（ＳＲ

ＥＳ）を、Ａ３アリゴリズムを使用して計算する（ステップ１３１４）。ステップ１３１６において、ＳＩＭプロセッサ３５ａは、空中インターフェース暗号化キーＫｃを、ランダム数（ＲＡＮＤ１）および端末キーKaを使用して計算する。ステップ１３１８において、ＳＩＭ３５は、署名された応答数（ＳＲＥＳ）と空中インターフェース暗号化キー（Ｋｃ）とを、カードリーダー装置３３を介して、端末プロセッサ３７に送信する。

【００８３】次に、ＳＩＭ３５は、図１４の処理を実行する。図２４を参照すると、署名された応答数（ＳＲＥＳ）のステップ１０１８における受信時に、端末プロセッサ３７は、ＳＲＥＳ数を地球局６ａに送信する（ステップ１０２０）。図２５を参照すると、地球局６は、署名された応答数を受信し（ステップ１１１４）、かつ、署名された応答数を、（３連レジスタ４８２内に収容された）記憶された署名された応答数と比較する。もし、２つの応答数が一致しないならば、呼は終了される（ステップ１１１７）。この他に、もし、望まれるならば、識別検証におけるさらなる試みが行われる。

【００８４】もし、ステップ１１１６において、移動端末２から受信された署名された応答が、記憶された署名された応答と一致するならば、地球局６は、ちょうど受信された署名された応答に対応する３連レジスタ４８２に記憶された暗号化キーＫｃを読み、かつ、移動端末２への全ての以降の信号を暗号化することと、移動端末２からの全ての以降の信号を解読することとを、暗号化キーＫｃと共にＡＳアリゴリズムを使用して、開始する（ステップ１１１８）。ＧＳＭシステムにおいて従来的であるように、フレーム番号は、また、暗号化アリゴリズムへの入力として使用される。その後、地球局６は、データベース局１５から受信される部分キーKpaを端末２ａに送るために、図１２のステップ１１０８へ戻る。しかし、この実施形態において、このことは、暗号化された形式で実施する。

【００８５】図２４に戻ると、ＳＩＭ３５からの空中インターフェース暗号化キーＫｃの受信時（ステップ１０２２）に、端末プロセッサ３７は、暗号化／解読モードを開始する。暗号化／解読モードでは、Ａ５アリゴリズムと空中インターフェース暗号化キーＫｃとを使用して、空中インターフェースモデム３２から受信される全てのトラフィックが解読され、かつ、空中インターフェースモデム３２へ送信される全てのトラフィックが暗号化される。さらに、地球局６がフレーム番号を使用すると、端末２は、同様に、フレーム番号を使用する。そして、（この例における）端末２ａの端末プロセッサ３７によって実行される処理は、地球局６から受信された部分暗号化キーKpaを、（暗号化された形式で）受信し、かつ、解読し、かつ、使用するために、図１１のステップ１００４へ戻る。対応する処理は、端末２ｂに対して、実行される。

【００８６】上記記載は、端末は新たには識別検証されないということ、および、端末は既に空中インターフェース暗号化モードにあるわけではない、ということを仮定しているが、このことは必ずしもそうである必要はない。もし、どちらかの端末が、空中インターフェース暗号化を、既に適用しているならば、識別検証および空中インターフェース暗号化を設定するための上記対応するステップは、再度実行されるわけではない。上記実施形態では、追加の保護が設けられる。例えば、安全な通信を開始するために、端末使用者は、ＳＩＭ上に収容されたデータと照合するためのＰＩＮコードを入力することを要求される。本発明がＧＳＭ互換システムまたは同様のシステムで実行される場合、ＳＩＭ３５は、国際移動加入者識別番号（ＩＭＳＩ）の形式で、さらなる情報を含み、かつ、高速ダイヤルまたは他の目的のための電話番号のリストを選択的に含む。

【００８７】●電話会議

本発明に従った暗号化計画は、各々の端末２ａ，２ｂで形成される共通暗号化／解読コードKRは、データベース局１５から供給されるランダム数（ＲＡＮＤ）からなる、という重要な優位性を有する。故に、本発明に従った方法では、暗号化／解読コードKRの長さは、呼の間に使用される端末の番号とは無関係である。このことは、図２８を参照してここで説明されるような電話会議を暗示している。この図は、図１０にほぼ対応しているが、電話会議での使用のために、２以上の使用者端末を図解している。図２８では、３つの端末（即ち、端末２ａ，２ｂ，２ｎ）が示されている。端末２ａ，２ｂ，２ｎは、それぞれ、地球局６ａ，６ｂ，６ｎと個別の通信リンクを形成している。

【００８８】電話会議を設定するために、部分キーKpa，Kpb，Kpnが、中央データベース局１５から、各々の地球局６ａ，６ｂ，６ｎに送信される。そして、これらのキーは、個々の使用者端末２ａ，２ｂ，２ｎに送信される。そして、部分キーは、使用者端末において個別に、各端末が共通暗号化コードKR＝（ＲＡＮＤ）を創り出すように先に説明された方法で、デコードされる。そして、端末は、３つの使用者端末の間の電話会議のためのデータを暗号化および解読するために、共通コードKRを使用できる。３つの端末が示されているが、もっと多くの端末が電話会議のために使用され得る。この方法は、我々の先の英国特許出願第９６１１４１１．１号で説明された方法（各端末が、呼のために使用される他の全ての端末に対する端末キーコードに基づくデータを提供される必要がある方法）とは対称的である。そのため、多くの端末が電話会議で使用される場合、暗号化コードは非常に長くかつ扱い難くなる。

【００８９】通常の２つのパーティの呼を３つのパーティの電話会議に拡張するために、または、電話会議内のパーティの数を増加するために、呼が進行中の間に、１

または２以上の追加の端末が呼に参加してもよい。この目的のために、参加しているパーティは、データベース局１５からのコードＲＡＮＤのマスクされたバージョンを、パーティ間で続いているデータ送信のためのフレーム番号と共に送る。それによって、参加しているパーティは、暗号化キーの現在の値を計算するために、かつ、送信されたデータの流れに参加するために、局所的に収容されたＡ５アリゴリズムを使用できる。

【００９０】多くの使用者端末の間の安全な電話会議を設定する能力は、安全な閉鎖使用者グループ（ＣＵＧ）のための特定の用途を有する。この目的のために、データベース局１５は、電話会議における他のメンバーと、または、個別に通信することを許可された閉鎖使用者グループのメンバーのリストを具備する。例えば、閉鎖使用者グループは、武装されたサービス者または緊急サービス者を具備してもよい。変更においては、特定の計画（例えば、組み合わされたサービス処理）に対して、ＣＵＧが、電話会議を通してまたは個々に、安全な暗号化された方法で、互いに通信できるように、２以上のデータベース局１５が設けられ、かつ、２以上のＣＵＧが（例えば一時的に）設備を共用することができるよう２以上のＣＵＧを調整するために、監督データベース局（図示略）が使用される。他の変更において、単一のデータベース局１５が使用され、かつ、共同の仮の周期の間、全ての使用者端末は、仮のグループ内での安全な通信を可能とするために、再プログラムされたＳＩＭカードが与えられる。

【００９１】●他の実施形態

先に説明された実施形態に対する多くの変更および他の形態は、当業者とって明白であり、かつ、本発明の範囲内である。例えば、実際に、異なるチャネル上の使用者端末間において、２重通信が起こる。追加の安全性のために、異なる個々のコードKRが、各々の２重通信のために使用され、各チャネルに対する疑似ランダム数（ＲＡＮＤ）の異なる値を使用して、データベース局１５から送信された個々の部分キーによって生成される。

【００９２】示される衛星と衛星軌道との数は単なる代表的なものである。より高い軌道において、より少ない数の（１または複数の）静止衛星が使用され得る。または、より多い数の低地球軌道（ＬＥＯ）衛星が使用され得る。同様に、中間軌道において、異なる数の衛星が使用され得る。ＴＤＭＡは、適したアクセスプロトコルとして説明されたが、符号分割多重アクセス（ＣＤＭＡ）または周波数分割多重アクセス（ＦＤＭＡ）のような他のアクセスプロトコルが使用され得る。本発明の原理は、衛星通信システムへ適用されるような上記のものとして予見されるが、他の通信システム（例えば、ＧＳＭのような、しかし、ＧＳＭには限定されないデジタル地上セルラーシステム）における本発明の使用もまた、可能である。

【００９３】便宜上のために、先の記載において、語句「移動」は端末２を示すために使用されたが、この語句は、携帯端末または可搬端末には限定されず、例えば、船舶または飛行機上に、または、地上車両に搭載された端末を含む。同様に、いくつかの完全に固定された端末２を伴って本発明を実施することが可能である。全ての端末装置２の詳細を記憶している単一の中央データベース局１５を設ける代わりに、同様の詳細が、その基地ゲートウエー８を登録する全ての端末装置に対する基地ゲートウエー８で記憶され得る。

【００９４】上述された実施形態において、中央データベース局１５は、ＧＳＭシステムの基地位置レジスタ（ＨＬＲ）として動作し、かつ、商業的に利用可能なＨＬＲハードウェアを使用して設けられ、かつ、各地球局６内のデータベースは、ビジッティング位置レジスタ（ＶＬＲ）の方法で動作し、かつ、同様に、商業的に利用可能なＧＳＭハードウェアを使用するが、異なる使用者に関する情報は、いくつかの異なるデータベース間に分配され得る。例えば、各閉鎖使用者グループに対する１つのデータベースが、物理的に異なる位置に存在できる。

【００９５】上記第４実施形態において、同一の端末キーKiが、空中インターフェース暗号化のために使用されるように、安全な端末相互暗号化のために使用されるが、このことは、必ずしも必要ではない。各端末は、２つの異なる端末キー（１つは空中インターフェース暗号化のためのものであり、もう１つは端末相互暗号化のためのものである）を記憶できる。この場合、識別検証中央データベースは、従来の空中インターフェース暗号化で使用される他に、端末相互暗号化キーの分配のために設けられ得る。

【００９６】先の実施形態では、ＧＳＭシステムの空中インターフェース暗号化のために使用される同一の（ＡＳ）暗号化アリゴリズムが、端末相互暗号化において使用されるが、異なる暗号化（この場合、端末は、第４実施形態における使用のための２つの異なる暗号化ステージを有する）が使用され得る。さらに、多数の閉鎖使用者グループが設けられる場合、各閉鎖使用者グループは、異なる暗号を使用できる。

【００９７】先において、ゲートウエー８は、実際には、ゲートウエーの機能を実行する追加の動作制御プログラムを設けることによって、ＩＳＣまたは交換または移動スイッチングセンター（ＭＳＣ）内に具備される。先において、専用地上ネットワーク線が説明され、かつ、好まれている。しかしながら、ＰＳＴＮまたはＰＬＭＮリンクの使用は排除されない。ＰＳＴＮまたはＰＬＭＮでは、例えば、賃貸線が利用不可能である。または、ＰＳＴＮまたはＰＬＭＮでは、トラフィックを処理するために、仮の追加容量が要求される。

【００９８】もし、ゲートウエー８内の記憶装置とゲー

トウエー８の他の構成要素とが、信号送信リンクを介して接続されているならば、ゲートウエー８内の記憶装置は、ゲートウエー８の他の構成要素と物理的に共に配置される必要はない。先において、語句「グローバル」が使用され、かつ、衛星システムが地球の全体または十分な部分をカバーすべきことが好まれるが、本発明は、また、（例えば、１または２以上の大陸の）さらに限定された範囲を伴う同様のシステムに拡張する。

【００９９】先の説明は２重通信システムを説明するが、本発明は、１地点対多地点または同報通信システムのような単信方式の（一方向の）送信システムに、同様に適用可能である。先の説明された実施形態は直接送信システムであるが、本発明は、蓄積送信通信システムに適用可能である。蓄積送信通信システムでは、１つのパーティは、記憶および次に起こる（他のパーティへの）後の送信のために、メッセージを送信する。

【０１００】そのような蓄積送信システムの一例は、例えば、Compuserve（登録商標）またはMCI（登録商標）によって提案される型の電子メール（e-mail）である。他の例は、インターネットである。インターネットは、よく知られているとおり、多数のホストコンピュータサイトからなる。このホストコンピュータは、高速パケット送信リンクのバックボーンによって相互接続され、かつ、公衆遠距離通信または他のネットワークを介して、世界の大抵の地点からのファイルの移動に対してアクセス可能である。

【０１０１】この型の実施形態では、中央データベース局１５は、両方の端末に同時にキーを分配する必要がない。代わりに、送信端末への部分キーの分配は、暗号化された形式で記憶するためのデータのファイルの送信の時点で起こり、かつ、受信端末への部分キーの分配は、例えば、受信端末がネットワークに接続される次の機会に、および／または、ファイルをホストコンピュータ内の中間記憶装置からダウンロードすることを、受信端末が要求する次の機会に、続いて後に起こる。

【０１０２】先に説明された実施形態は音声送信に関するが、本発明は、いかなる種類のデータ、特に（それだけに限定されるわけではないが）イメージデータや映像データやテキストファイルや同様のデータ、の暗号化にも適用可能である。本発明の様々な構成要素の地理的位置は重要ではない。上記実施形態のシステムの異なる部分は、異なる国の管轄区域に設けられてもよい。本発明は、本発明の概念に貢献する遠距離通信装置およびシステムのいかなる部分または構成要素にも拡張する。

【図面の簡単な説明】

【図１】　本発明を具体化する通信システムの構成要素を概要的に示すブロック図である。

【図２】　本発明を伴った使用に適した移動端末装置の構成要素を概要的に示すブロック図である。

【図３】　図１の実施形態の一部を形成する地球局ノードの構成要素を概要的に示すブロック図である。

【図４】　図１の実施形態の一部を形成するゲートウエー局の構成要素を概要的に示すブロック図である。

【図５】　図１の実施形態の一部を形成するデータベース局の構成要素を概要的に示すブロック図である。

【図６】　図５のデータベース局の一部を形成する記憶装置の内容を図解する説明図である。

【図７】　図１の実施形態において、衛星によって生成されるビームを概要的に図解する説明図である。

【図８】　地球の周りの軌道において、図１の一部を形成する衛星の配置を概要的に図解する説明図である。

【図９】　本発明の第１実施形態において、図２の送受器の構成要素間における信号の流れを示すブロック図である。

【図１０】　第１実施形態において、図１の構成要素間における暗号化データおよび信号の流れを示す概要的なブロック図である。

【図１１】　第１実施形態において、図９の送受器の制御および暗号化構成要素によって実行される処理を概要的に示す流れ図である。

【図１２】　第１実施形態において、図３の地球局の動作の処理を概要的に示す流れ図である。

【図１３】　第１実施形態において、図４の中央データベース局の動作の処理を概要的に示す流れ図である。

【図１４】　第１実施形態において、図９の送受器内に収容された加入者情報モジュール（ＳＩＭ）の動作の処理を概要的に示す流れ図である。

【図１５】　本発明の第４実施形態で提供された安全性のステージを概要的に図解する流れ図である。

【図１６】　図９の第１送受器端末による暗号化キーの形成のステージを示す説明図である。

【図１７】　第２送受器における暗号化キーの形成の処理を示す説明図である。

【図１８】　本発明の第３実施形態において、図１３および図１４の流れ図の動作を変更する流れ図である。

【図１９】　本発明の第３実施形態において、図１３および図１４の流れ図の動作を変更する流れ図である。

【図２０】　本発明の第４実施形態において、空中インターフェース暗号化および識別検証システムの組み合わせの一例を示す流れ図である。

【図２１】　本発明の第４実施形態に従った図９の送受器内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。

【図２２】　第４実施形態のデータベース局内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。

【図２３】　第４実施形態の地球局内に存在する機能的な構成要素のうちのいくつかを概要的に示すブロック図である。

【図２４】　第４実施形態に従った送受器の動作を概要

29

的に示す流れ図である。

【図２５】　第４実施形態に従った地球局の動作の処理を概要的に示す流れ図である。

【図２６】　第４実施形態に従ったデータベース局の動作を概要的に示す流れ図である。

【図２７】　第４実施形態に従った加入者情報モジュールの動作を概要的に示す流れ図である。

【図２８】　本発明の実施形態が、３以上の使用者端末を伴う電話会議のために、どのように使用され得るのかを図解する説明図である。

【符号の説明】

30

２ａ，２ｂ……移動使用者端末装置

４ａ，４ｂ……軌道周回中継衛星

６ａ，６ｂ……衛星地球局ノード

８ａ，８ｂ……衛星システムゲートウエー局

１０ａ，１０ｂ……公衆交換遠距離通信ネットワーク

１２ａ，１２ｂ……固定遠距離通信端末装置

１５……端末位置データベース局

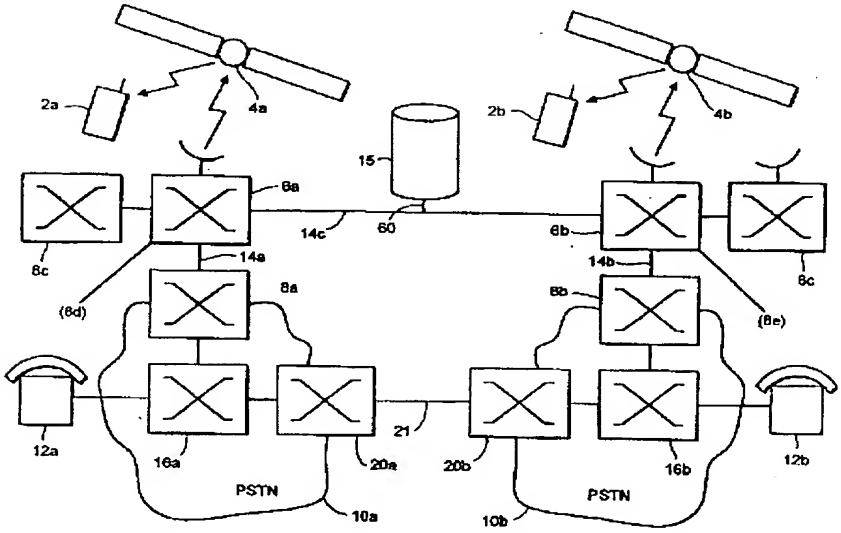
１６ａ，１６ｂ……局所交換機

２０ａ，２０ｂ……国際スイッチングセンター

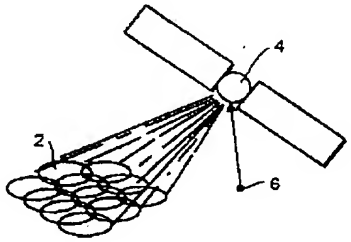
10　２１……トランスナショナルリンク

６０……信号送信リンク

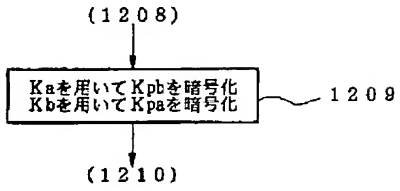
【図１】



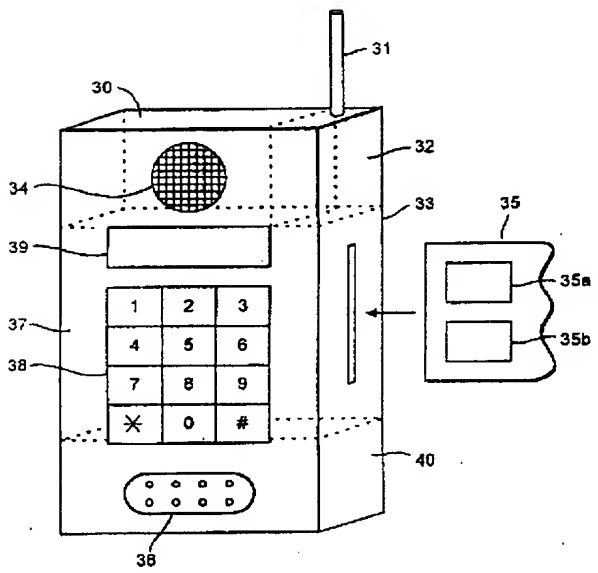
【図７】



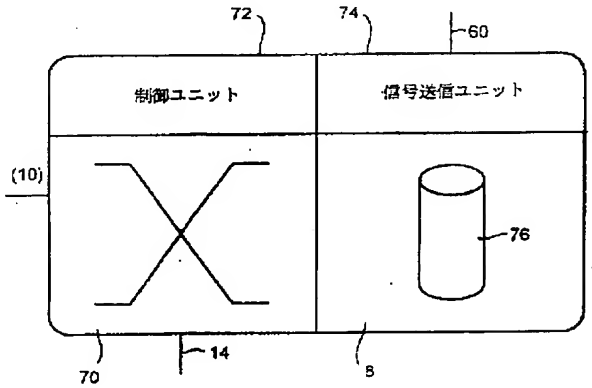
【図１８】



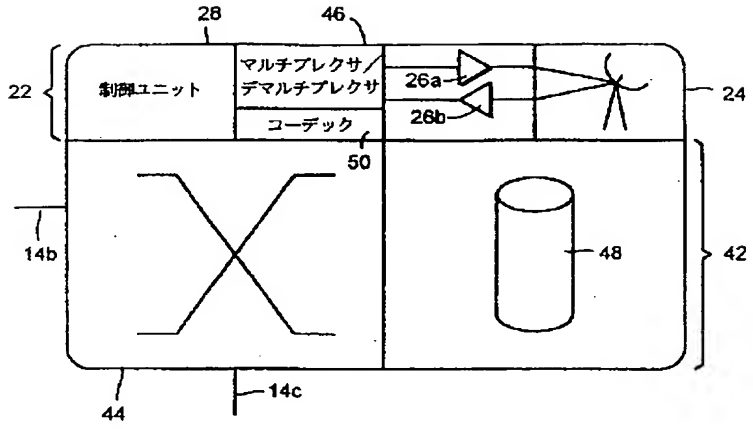
【図２】



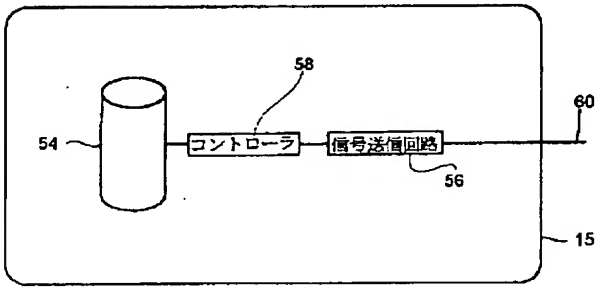
【図４】



【図３】



【図５】

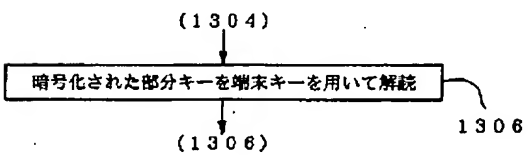


【図６】

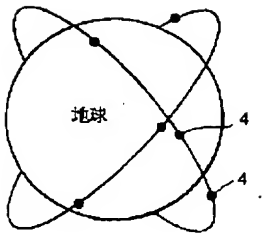
54

ID #	キーKi	状態	位置	有効ノード	利用可能?	基地
00001	K_A	ローカル	46°, 35°	6a	Y	8a
00002	K_B	グローバル	71°, 27°	6b	Y	8b

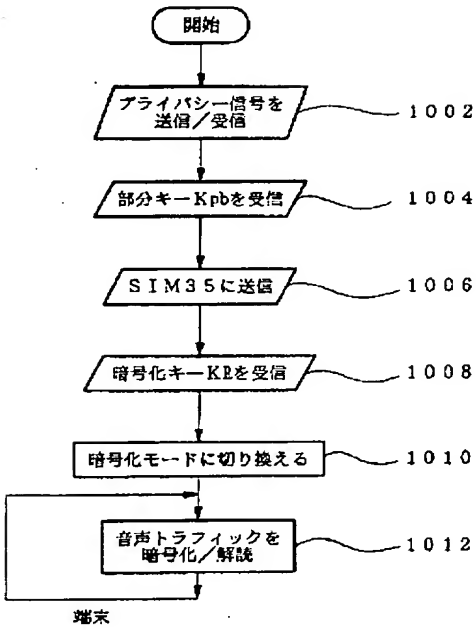
【図１９】



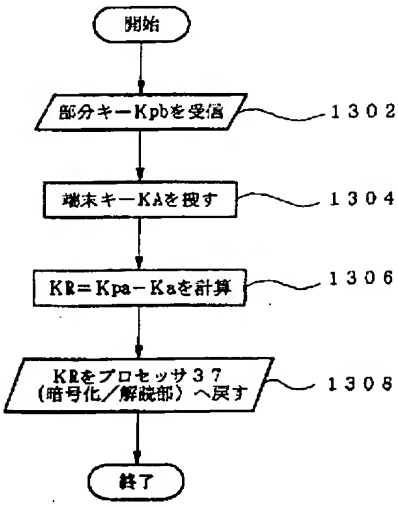
【図８】



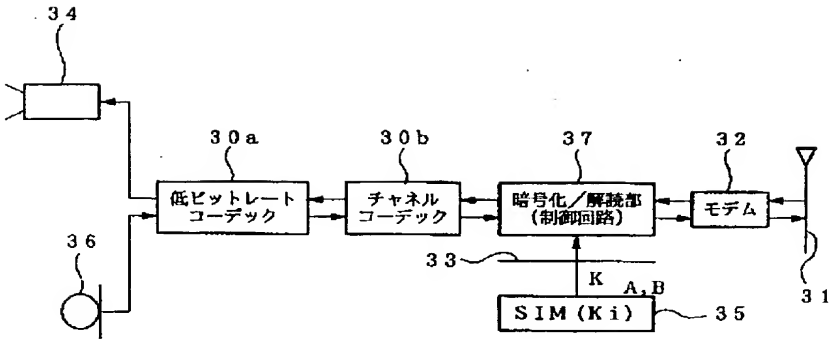
【図１１】



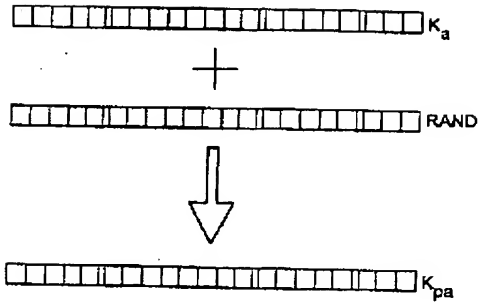
【図１４】



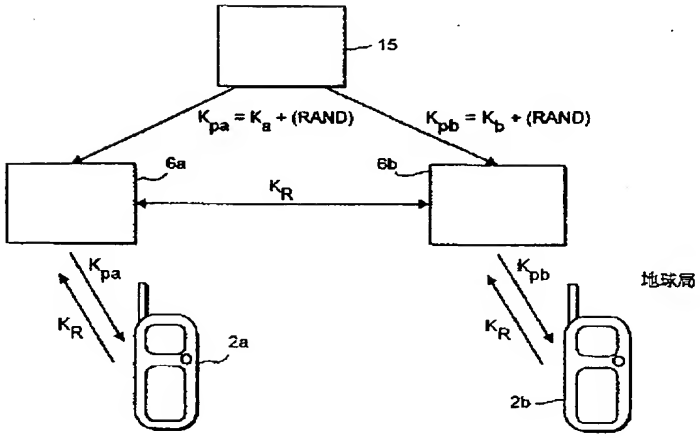
【図９】



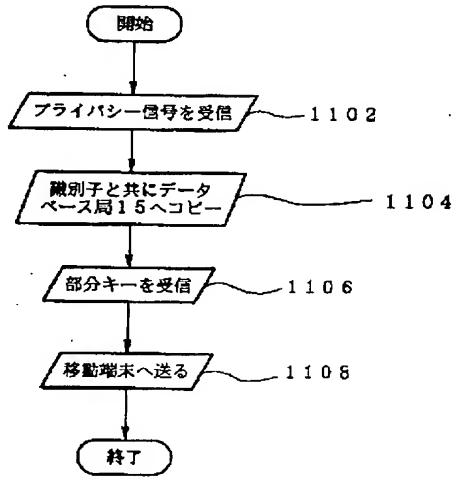
【図１６】



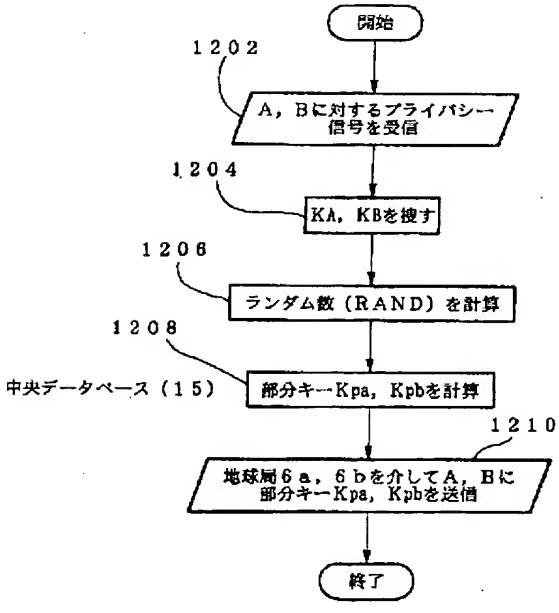
【図１０】



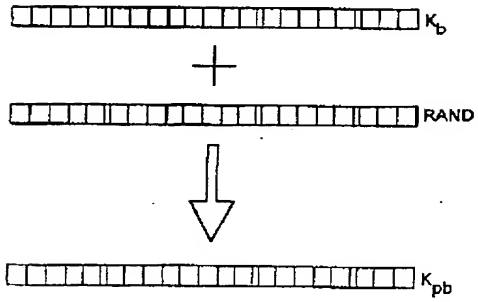
【図１２】



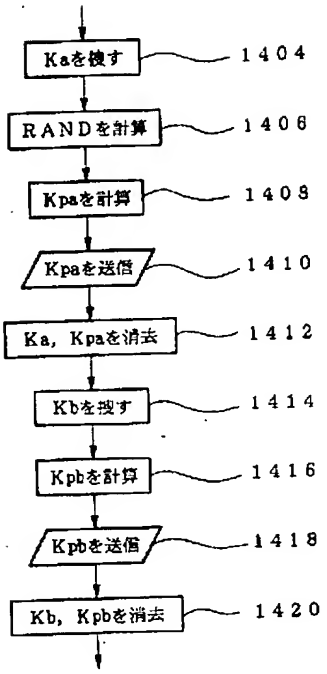
【図１３】



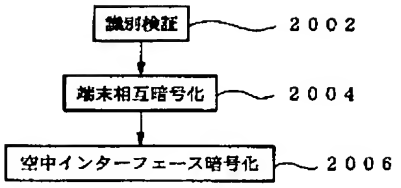
【図１７】



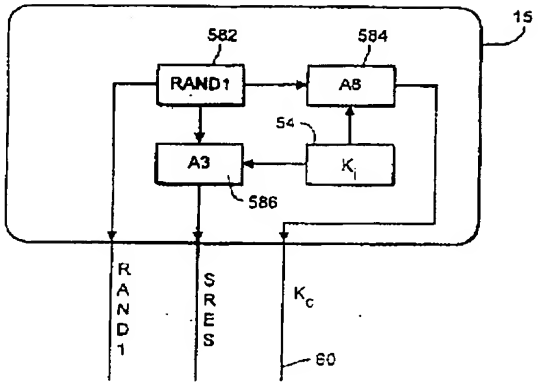
【図１５】



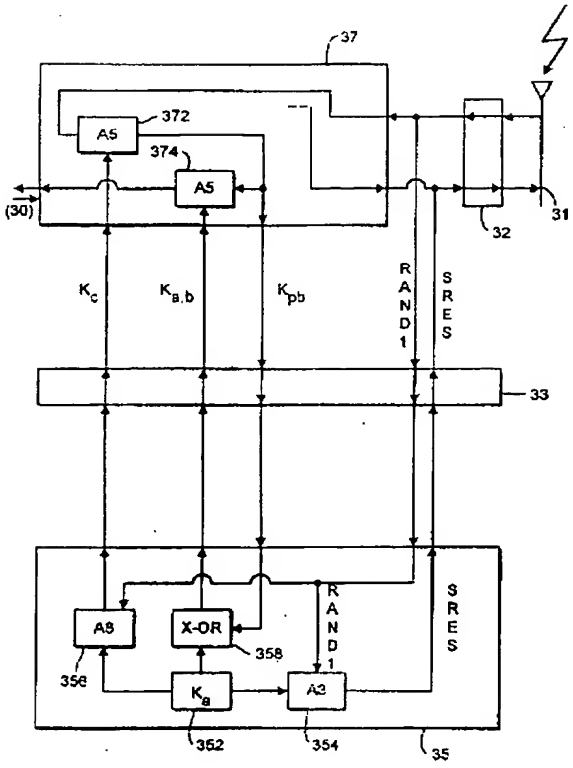
【図２０】



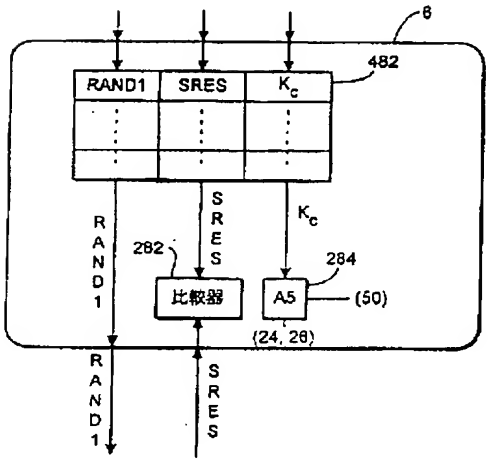
【図２２】



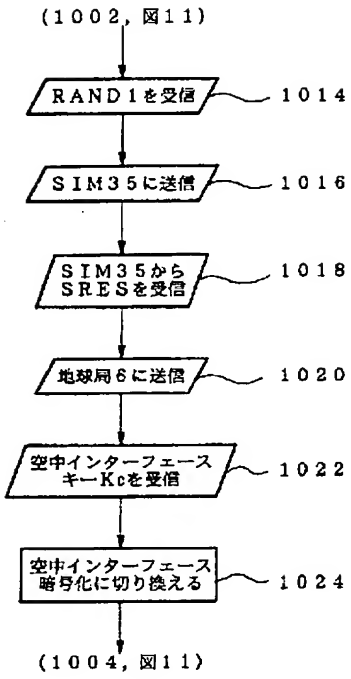
【図２１】



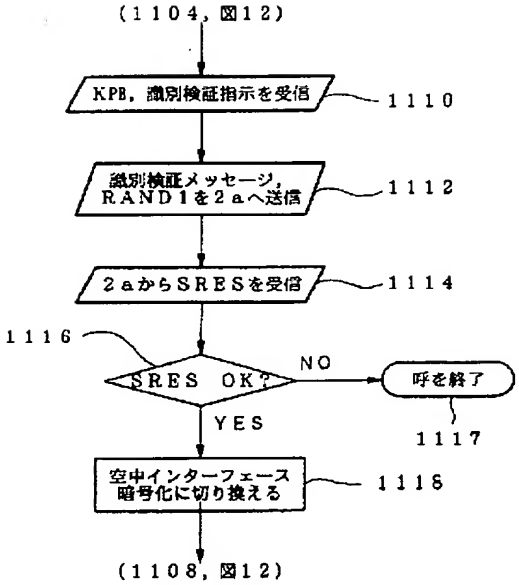
【図２３】



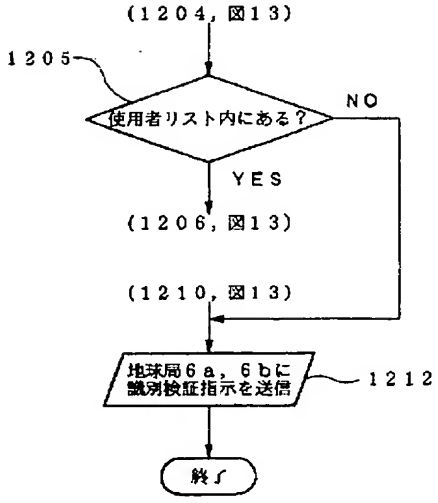
【図２４】



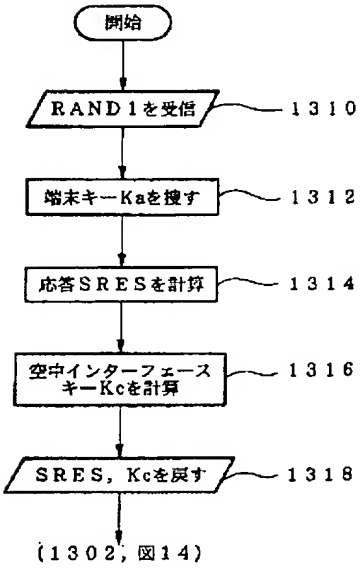
【図２５】



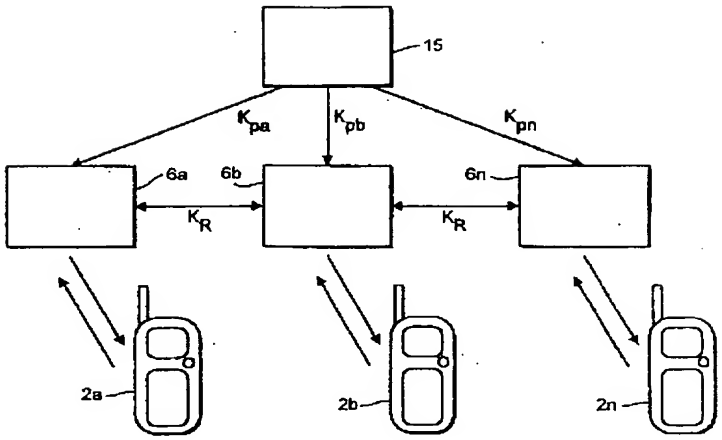
【図２６】



【図２７】



【図２８】



【外国語明細書】

1 Title of Invention

Communication Security

2 Claims

1. A method of distributing through a communications network, enciphering key data to be used in encrypting and decrypting data at first and second terminals (2_a, 2_b) so as to provide secure data transmission between the terminals through the network, the terminals each storing corresponding first and second terminal keys (K_a, K_b), the method comprising:

storing the first and second keys (K_a, K_b) remotely of the terminals (2_a, 2_b);

generating at a location remote from both of the terminals, first and second separate partial keys (K_{pa}, K_{pb}) each as a masked function of a common number (RAND) and a corresponding one of said stored keys (K_a, K_b);

dispatching the first partial key (K_{pa}) separately towards the first terminal (2_a); and

separately dispatching the second partial key (K_{pb}) towards the second terminal (2_b).

「以下 余白」

2. A method according to claim 1 wherein the enciphering key data is to be used for encrypting and decrypting data at said first and second terminals (2_a, 2_b) and at least one further terminal (2_n) so as to provide security for concurrent data transmissions between all of said terminals (2_a, 2_b, 2_n) through the network, the method further including:

storing a further key (K_n) remotely of the terminals (2_a, 2_b, 2_n) corresponding to the terminal key of the further terminal (2_n);

generating a further partial key (K_{pn}) as a masked function of the common number (RAND) and said remotely stored further key (K_n); and

dispatching the further partial key (K_{pn}) towards the further terminal (2_n).

3. A method according to claim 2 including causing the further terminal to join in data transmission between the terminals whilst said transmission is in progress, including transmitting to the further terminal, timing data

「以下 余白」

concerning the data transmission between the terminals.

4. A method according to any preceding claim including generating said partial keys with said common number (RAND) only for a predetermined group (CUG) of said terminals (2) to provide for secure communication between the terminals of the group.

5. A method of setting up a first terminal (2_a) that stores an individual terminal key (K_a), to encrypt data to be transmitted according to a secure encryption code (K_R) through a communications network to a second terminal (2_b) where the data is to be decrypted, comprising:

receiving at the first terminal a partial key (K_{pa}) dispatched thereto through the network from a remote location, the partial key being a masked function of the individual terminal key (K_a) and a number (RAND) for determining the encryption code; and

comparing at the terminal (2_a)the received partial key (K_{pa}) and the stored key (K_a) so as to provide the encryption code (K_R).

6. A method according to claim 5 including encrypting data at the first terminal (2_a) according to the encryption code (K_R), and transmitting the encrypted data towards the second terminal through the network.

7. A method of setting up a second terminal that stores an individual terminal key (K_b), to decrypt data transmitted thereto according to a secure encryption code through a communications network from a first terminal where the data is encrypted, comprising:

receiving at the second terminal a partial key (K_{pb}) dispatched thereto through the network from a remote location, the partial key being a masked function of the individual terminal key (K_b) and a number (RAND) for determining the code; and

comparing at the terminal the received partial key (K_{pb}) and the stored key (K_a) so as to provide data (K_R) for decrypting data transmitted from the

first terminal and encrypted according to the encryption code (K_R).

8. A method according to claim 7 including decrypting data at the second terminal, transmitted thereto from the first terminal and encrypted according to the encryption code (K_R).

9. A method according to any preceding claim wherein the or each said partial key (K_{pa}, K_{pb}, K_{pn}) is transmitted to the terminals (2_a, 2_b, 2_n) over the air interface of a mobile communications system.

10. A method according to claim 9 including additionally encrypting data transmitted over the air interface.

11. A method according to claim 10 including performing the additional encryption at each said terminal with the terminal key of the respective terminal and a predetermined algorithm.

12. Apparatus (15) for distributing through a communications network, enciphering key data to be used in encrypting and decrypting data at first and second terminals (2_a, 2_b) so as to provide secure data transmission between the terminals through the network, the terminals each storing corresponding first and second terminal keys (K_a, K_b), comprising:

a data store disposed remotely of the terminals (2_a, 2_b), storing first and second terminal keys (K_a, K_b) corresponding to the terminal keys stored by the terminals respectively;

means for generating a number (RAND);

means for generating first and second separate partial keys (K_{pa}, K_{pb}) each as a masked function of the number (RAND) and a corresponding one of said keys (K_a, K_b) held in the store; and

dispatching means operative to dispatch the first partial key (K_{pa}) towards the first terminal (2_a) and the second partial key (K_{pb}) separately towards the second terminal (2_b).

13. A terminal (2_a, 2_b, 2_n) for communicating through a communication network with at least one further terminal, comprising

means to receive a store (SIM) that stores an individual terminal key (K_i),

a key generator (35a) to receive from the network a partial key (K_{ri}) comprising a masked function of the individual terminal key (K_i) and number (RAND) transmitted in common to said least one further terminal, and operative to compare the individual key stored in the store (SIM) with said partial key so as produce an encryption code (K_R) as a function of said number (RAND); and

enciphering means (37) operative to encipher data transmitted through the network in accordance with the encryption code (K_R).

14. A terminal according to claim 13 including user operable means (38) for selectively initiating operation of the enciphering means.

15. A terminal according to claim 13 or 14 operative to transmit and receive data in different channels through the network, wherein the enciphering means (37) is operative to encipher data transmitted through the network in accordance with a first said encryption code (K_R), and including deciphering means (37) operative to decipher data received through the network in accordance with a second, different said encryption code (K_R).

「以下 余白」

3 Detailed Description of Invention

Field of the invention

This invention relates to a method and apparatus for providing secure communication through a communications network.

Background

Digital mobile voice communications systems are well known and one example is the GSM terrestrial cellular system. Others are the Inmarsat-M satellite telephone system, the IRIDIUM ™ satellite cellular system described in, for example, EP-A-0365885, the ICO ™ satellite cellular system described in, for example, GB-A-2295296 or the ODYSSEY ™ satellite cellular system described in, for example EP-A-0510789. Since such systems operate over a wireless link, there is a risk of interception of calls by unauthorised persons.

The GSM system includes an optional encryption scheme described in, for example, "Security aspects and the implementation in the GSM-system"; Peter C.J. van der Arend, paper 4a, Conference Proceedings of the Digital Cellular Radio Conference (DCRC), October 12th-14th 1988, published by Deutsche Bundespost, France Telecom and Fernuniversitat. Greater detail is given in the following GSM recommendations: GSM 02.09 "Security Aspects"; GSM03.20 "Security Related Algorithms". In this scheme, a database known as the Authentication Centre (AuC) holds an individual encryption key number (K_i) for each subscriber to the authentication service, which is also stored on a chip known as the Subscriber Information Module (SIM) held in the subscriber's mobile terminal. The subscriber has no access to the data stored in the SIM and cannot read the key.

Where a secure session is requested, a random number (RAND) is generated by the AuC and used, together with the customer's key (K_i), to calculate a ciphering key (K_c) used during the session for ciphering and deciphering messages to/from the subscriber. The random number is sent from the AuC

「以下 余白」

to the subscriber's mobile terminal via the Base Transceiver Station (BTS). The mobile terminal passes the random number to the SIM, which calculates the ciphering key K_C using an algorithm termed A5, from the received random number and the stored key (K_i). Thus, the random number is sent over the air, but not the customer's key K_i or the ciphering key K_c.

The random number and the ciphering key K_c are fed to the Home Location Register (HLR) database of the GSM network, which stores details for the subscriber concerned, and are also sent to the Visiting Location Register (VLR) for the area where the user terminal is currently located, and are supplied to the BTS via which the mobile is communicating to the network.

The ciphering key K_c is used, together with the current TDMA frame number,to implement the A5 ciphering algorithm in both the mobile terminal and the BTS so that data transmitted over the air interface between the mobile terminal and the BTS is encrypted. Thus, the individual user key K_i is stored only at the authentication centre and the SIM, where the ciphering key K_c is calculated and forwarded to the BTS and the mobile terminal.

Whilst this scheme is adequate in many respects, it fails to provide complete security since it offers protection only over the air transmission path. Thus, it is possible for illicit access to be obtained by tampering with the fixed part of the network.

Accordingly, end-to-end encryption schemes have been proposed. Because the encryption runs from one user terminal to the other, across the whole communications path and not just the air path, improved privacy is obtained.

The basic problem in offering end-to-end encipherment of communications over a network is in providing each of the two users with the same, or each other's, secret key. In some applications, a group of terminals (for example all owned by a single body) may all have access to the same key. Whilst this

provides privacy against personnel from outside the group, it is an incomplete solution since it does not provide privacy for communication between two terminals within the group and a third within the group.

It is possible to employ public key encryption systems, in which each terminal has a secret decryption key and a non-secret encryption key, so that any other party can use the encryption key to encrypt data but only the recipient can decrypt data which has been encrypted using the public encryption key.

A communication system could be envisaged in which every user is provided with such a pair of keys, and in setting up a communication between a pair of users each sends the other its encryption key whilst keeping its decryption key secret. However, there is widespread public concern that the use of such techniques on a telecommunications network would allow criminals or terrorists to communicate using completely secure communications, free from any possibility of supervision.

It has been proposed to hold the keys in a remote "trusted third party" database. An example of such an arrangement is described in "Security measures in communication networks", K. Presttun, Electrical Communication, 1986, Vol 60, No. 1 pp 63-70. The keys for two users (user A and user B) are distributed from a remote key distribution centre as a common, masked message, which is firstly sent to user A, where the key for user A is stripped out, and then from user A to user B, to provide the key to user B.

In our GB 96 11411.1 (and corresponding USSN 08/866 912) there is described an end-to-end encryption and decryption scheme in which the terminal keys that are stored in the terminals, are held additionally in a remote "trusted third party" database. In order to set up an encrypted transmission between a first and a second terminal, each of them is provided

from the remote location with a partial key which contains masked data concerning the key of the other terminal, derived from the stored data in the database. As a result, both terminals can be provided with data that in combination with their own key stored at the terminal, enables them each to set up a common secret code which can be used for end to end encryption and decryption through the network.

A difficulty with the prior references "trust third party" databases arises when it is desired to set up secure conference calls between three or more terminals. Each terminal needs to be provided with masked data concerning all the keys of the other terminals participating in the conference call so that they can each establish a common code, with the result that the partial keys and the final encryption code become long and cumbersome in dependence upon the number of participants. Also the risk of the code being ascertained by eavesdropping, from the long partial keys, is increased.

Summary of the invention

The present invention provides a solution to these problems. The invention provides a method of distributing through a communications network, enciphering key data to be used in encrypting and decrypting data at first and second terminals so as to provide secure data transmission between the terminals through the network, the terminals each storing corresponding first and second terminal keys, the method comprising: storing the first and second keys remotely of the terminals; generating at a location remote from both of the terminals, first and second separate partial keys each as a masked function of a common number and a corresponding one of said separately stored keys; dispatching the first partial key separately towards the first terminal; and separately dispatching the second partial key separately towards the second terminal.

The invention also provides a method of setting up a first terminal that stores an individual terminal key, to encrypt data to be transmitted according to a

secure encryption code through a communications network to second terminal where the data is to be decrypted, comprising receiving at the first terminal a partial key dispatched thereto through the network from a remote location, the partial key being a masked function of the individual terminal key and a number for determining the encryption code, and comparing at the terminal the received partial key and the stored key so as to provide the encryption code.

The invention also extends to a method of setting up a second terminal that stores an individual terminal key, to decrypt data transmitted thereto according to a secure encryption code through a communications network from a first terminal where the data is encrypted, comprising receiving at the second terminal a partial key dispatched thereto through the network from a remote location, the partial key being a masked function of the individual terminal key and a number for determining the code, and comparing at the second terminal the received partial key and the stored key so as to provide data for decrypting the code.

Thus in accordance with the invention, each terminal is provided with a partial key from the remote location that includes masked data concerning the terminal key of the terminal itself, without the need for key of the other terminal, so that the protocol can readily be expanded from communications between two terminals, to large numbers of terminals in conference calls without lengthening the partial keys.

One or more additional terminals may join in a call whilst it is in progress, either to expand a normal two party call into a three party conference call or to increase the number of parties in a conference call. To this end, the joining party is sent a masked version of its key so that it can determine the code, together with the frame number for the data transmission that is going on between the parties, so that the joining party can join in the transmitted data flow .

The invention is envisaged for use in satellite mobile digital communications systems, and is also useful in corresponding terrestrial digital mobile communication systems (e.g. in cellular systems such as the GSM system), or in fixed link communication systems. The invention may also be practised in store-and-forward communication systems such as e-mail or the Internet.

Brief description of the drawings

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram showing schematically the elements of a communication system embodying the present invention;

Figure 2 is a block diagram showing schematically the elements of mobile terminal equipment suitable for use with the present invention;

Figure 3 is a block diagram showing schematically the elements of an Earth station node forming part of the embodiment of Figure 1;

Figure 4 is a block diagram showing schematically the elements of a gateway station forming part of the embodiment of Figure 1;

Figure 5 is a block diagram showing schematically the elements of a database station forming part of the embodiment of Figure 1;

Figure 6 illustrates the contents of a store forming part of the database station of Figure 5;

Figure 7a illustrates schematically the beams produced by a satellite in the embodiment of Figure 1;

Figure 7b illustrates schematically the disposition of satellites forming part of Figure 1 in orbits around the earth;

Figure 8 is a block diagram showing the signal flow between components of the handset of Figure 2 in a first embodiment of the invention;

Figure 9 is a schematic block diagram showing the flow of encryption data and signals between the components of Figure 1 in the first embodiment;

Figure 10 is a flow diagram showing schematically the process performed by the control and enciphering components of the handset of Figure 8 in the first embodiment;

Figure 11 is a flow diagram showing schematically the process of operation of the earth station of Figure 3 in the first embodiment,

Figure 12 is a flow diagram showing schematically the process of operation of the central database station of Figure 4 in the first embodiment;

Figure 13 is a flow diagram showing schematically the process of operation of a subscriber information module (SIM) held within the handset of Figure 8 in the first embodiment;

Figure 14 is a flow diagram illustrating schematically the stages of security provided in a fourth embodiment of the invention;

Figure 15 is a an illustrative diagram showing the stages of formation of the enciphering key by a first handset terminal of Figure 8; and

Figure 16 is a corresponding illustrative diagram showing the process of formation of the enciphering key at a second such handset;

Figures 17a and b is a flow diagram modifying the operation of that of Figures 12 and 13 in the third embodiment of the invention;

Figure 19a is a block diagram showing schematically some of the functional elements present in the handset of Figure 8 according to the fourth embodiment of the invention;

Figure 19b is a block diagram showing schematically some of the functional elements present in the database station of the fourth embodiment,

Figure 19c is a block diagram showing schematically some of the functional elements present in the earth station of the fourth embodiment;

Figure 20 (incorporating parts of Figure 10) is a flow diagram showing schematically the operation of a handset according to the fourth embodiment;

Figure 21 (incorporating parts of Figure 11) is a flow diagram showing schematically the process of operation of an earth station according to the fourth embodiment;

Figure 22 (incorporating parts of Figure 12) is a flow diagram showing schematically the operation of a database station according to the fourth embodiment;

Figure 23 (incorporating parts of Figure 13) is a flow diagram showing schematically the operation of a subscriber information module according to

the fourth embodiment; and

Figure 24 illustrates how embodiments of the invention can be used for conference calls with more than two user terminals.

Detailed description

Referring to Figure 1, a satellite communications network according to this embodiment comprises mobile user terminal equipment 2a, 2b; orbiting relay satellites 4a, 4b, 4c; satellite earth station nodes 6a, 6b, 6c; satellite system gateway stations 8a, 8b; public switched telecommunications networks 10a,10b; and fixed telecommunications terminal equipment 12a,12b.

Interconnecting the satellite system gateways 8a, 8b, 8c with the earth station nodes 6a, 6b, 6c and interconnecting the nodes 6a, 6b, 6c with each other, is a dedicated ground-based network comprising channels 14a,14b,14c. The satellites 4, earth station nodes 6 and lines 14 make up the infrastructure of the satellite communications network, for communication with the mobile terminals 2, and accessible through the gateway stations 8.

A terminal location database station 15 is connected, via a signalling link 60 (e.g.within the channels 14 of the dedicated network) to the gateway station and earth stations 6.

The PSTNs 10a, 10b comprise, typically, local exchanges 16a, 16b to which the fixed terminal equipment 12a, 12b is connected via local loops 18a, 18b; and international switching centres 20a, 20b connectable one to another via transnational links 21 (for example, satellite links or subsea optical fibre cable links). The PSTNs 10a, 10b and fixed terminal equipment 12a, 12b (e.g telephone instruments) are well known and almost universally available today.

Each mobile terminal apparatus is in communication with a satellite 4 via a full duplex channel (in this embodiment) comprising a down link channel and

an up link channel, for example (in each case) a TDMA time slot on a particular frequency allocated on initiation of a call, as disclosed in patent applications
GB 2288913 and GB 2293725. The satellites 4 in this embodiment are non geostationary and thus, periodically, there is hand over from one satellite 4 to another.

Mobile terminal 2

Referring to Figure 2, the mobile terminal equipment of Figure 1 is shown. One suitable form is a handset, as shown. Details of the handsets 2a,2b etc will not be described and are similar to those presently available for use with the GSM system, comprising a digital coder/decoder 30, together with conventional microphone 36, loudspeaker 34, battery 40, keypad components 38, a radio frequency (RE) interface 32 and antenna 31 suitable for satellite communications. Preferably a display 39, for example a liquid crystal display, is also provided. A 'smart card' reader 33 receiving a smart card (SIM) 35 storing user information is also provided.

The coder/decoder (codec) 30 comprises a low bit rate coder, generating a speech bit stream at around 3.6 kilobits per second, together with a channel coder applying error correcting encoding, to generate an encoded bit stream at a rate of 4.8 kilobits per second. The low bit rate coder may, for example, be a linear predictive coder such as a multiple pulse predictive coder (MPLPC), a code book excited linear predictive coder (CELP), or a residual excited linear predictive coder (RELP). Alternatively, it may employ some form of waveform coding such as subband coding.

The error protection encoding applied may employ block codes, BCH codes, Reed-Solomon codes, turbo codes or convolutional codes. The codec 30 likewise comprises a corresponding channel decoder (e.g. using Viterbi or soft decision coding) and speech decoder.

Also provided is a control circuit 37 which may in practice be integrated with the coder 30, consisting of a suitably programmed microprocessor, microcontroller or digital signal processor (DSP) chip.

The SIM 35 preferably complies with GSM Recommendations 02.17 "Subscriber Identity Modules", and 11.11 and is preferably implemented as an industry standard "Smart Card". The SIM 35 and reader 33 are therefore preferably as described in International Standards ISO 7810, 7811 and 7816; these and GSM 02.17 and 11.11 are all incorporated herein by reference.

Specifically, the SIM 35 includes a processor 35a and permanent memory 35b. The processor 35a is arranged to perform some encryption functions as described in greater detail below.

Earth Station Node 6

The earth station nodes 6 are arranged for communication with the satellites.

Each earth station node 6 comprises, as shown in Figure 3, a conventional satellite earth station 22 consisting of at least one satellite tracking antenna 24 arranged to track at least one moving satellite 4 RF power amplifiers 26a for supplying a signal to the antenna 24, and 26b for receiving a signal from the antenna 24; and a control unit 28 for storing the satellite ephemeris data, controlling the steering of the antenna 24, and effecting any control of the satellite 4 that may be required (by signalling via the antenna 24 to the satellite 4).

The earth station node 6 further comprises a mobile satellite switching centre 42 comprising a network switch 44 connected to the trunk links 14 forming part of the dedicated network. A multiplexer 46 is arranged to receive switched calls from the switch 44 and multiplex them into a composite signal for supply to the amplifier 26 via a low bit-rate voice codec 50. The earth station node 6 also includes a local store 48 storing details of each mobile

terminal equipment 2a within the area served by the satellite 4 with which the node 6 is in communication.

Gateway 8

Referring to Figure 4, the gateway stations 8a,8b comprise, in this embodiment, commercially available mobile switching centres (MSCs) of the type used in digital mobile cellular radio systems such as GSM systems. They could alternatively comprise a part of an international or other exchange forming one of the PSTNs 10a, 10b operating under software control to interconnect the networks 10 with the satellite system trunk lines 14.

The gateway stations 8 comprise a switch 70 arranged to interconnect incoming PSTN lines from the PSTN 10 with dedicated service lines 14 connected to one or more Earth station nodes 6, under control of a control unit 72. The control unit 72 is capable of communicating with the data channel 60 connected to the database station 15 via a signalling unit 74, and is arranged to generate data messages in some suitable format (e.g. as packets or ATM cells).

Also provided in the gateway stations 8 is a store 76 storing billing, service and other information relating to those mobile terminals 2 for which the gateway station 8 is the home gateway station. Data is written to the store 76 by the control unit 72 after being received via the signalling unit 74 or switch 70, from the PSTN 10 or the Earth station nodes 6 making up the satellite nerwork. This store acts in the manner of a visitor location register (VLR) of a terrestrial GSM network, and a commercially available VLR may therefore be used as the store 76.

The satellite system trunk lines 14 comprise, in this embodiment, high quality leased lines meeting acceptable minimum criteria for signal degradation and delay. In this embodiment, all the lines 14 comprise terrestrial links. The trunk lines 14 are preferably dedicated lines, so that the lines 14 form a

separate set of physical channels to the networks 10. However, the use of virtual circuits through the networks 10 is not excluded.

Database Station 15

Referring to Figure 5, the database station 15 comprises a digital data store 54, a signalling circuit 56, a processor 58 interconnected with the signalling circuit 56 and the store 54, and a signalling link 60 interconnecting the database station 15 with the gateway stations 8 and Earth stations 6 making up satellite system network, for signalling or data message communications.

The store 54 contains, for every subscriber terminal apparatus 2, a record showing the identity e.g. the International Mobile Subscriber Identity or IMSI; the current status of the terminal 2 (whether it is "local" or "global" as will be disclosed in greater detail below); the geographical position of the mobile terminal 2 (either in co-ordinate geometry, or as code identifying an area within which it lies); the "home" gateway station 8 with which the apparatus is registered (to enable billing and other data to be collected at a single point) and the currently active Earth station node 6 with which the apparatus 2 is in communication via the satellite 4. The contents of the store are indicated in Figure 6.

Further, in this embodiment the store contains for each user a unique and individual enciphering key Ki, to be used as described below.

The signalling unit 56 and processor 58 are arranged to receive interrogating data messages, via the signalling circuit 60 which may be a packet switched connection, from gateways 8 or nodes 6, comprising data identifying one of the mobile terminals 2, for example, the telephone number of the equipment 2, and the processor 58 is arranged to search the store 54 for the status and active earth station node 6 of the terminal 2, and to transmit these in a reply message via the data line 60.

Thus, in this embodiment the database station 15 acts to fulfil the functions both of a home location register (HLR) of a GSM system, and of an authentication centre (AuC) of a GSM system, and may be based on commercially available GSM products.

Satellites 4

The satellites 4a, 4b comprise generally conventional communications satellites, such as the known Hughes HS 601 model, and may include features as disclosed in GB 2288913. Each satellite 4 is arranged to generate an array of beams covering a footprint beneath the satellite, each beam including a number of different frequency channels and time slots, as described in GB 2293725 and illustrated in Figure 7a.

The satellites 4 are arranged in a constellation in sufficient numbers and suitable orbits to cover a substantial area of the globe, preferably to give full, continuous global coverage. For example 10 or more satellites may be provided in two mutually orthogonal intermediate circular orbits at an altitude of, for example, 10,500 kilometres as shown in Figure 7b. However, larger numbers of lower satellites may be used, as disclosed in EP 0365885, or other publications relating to the Iridium system, for example.

Registration and Location

In one embodiment, a customer mobile terminal apparatus 2 may be registered with one of two distinct statuses; "local" in which the mobile terminal apparatus is permitted only to communicate through one local area, or part of the satellite system network, and "global", which entitles the apparatus to communicate through any part of the satellite system network.

The status of each apparatus 2, i.e. "local" or "global", is stored in the record held for the apparatus 2 concerned in the store 54 of the database station 15, as shown in Figure 6.

The mobile terminal apparatus 2 performs an automatic registration process, of the kind well known in the art of cellular terrestrial communications, on each occasion when the terminal 2 is utilised for an outgoing call; and/or when the apparatus 2 is switched on; and/or periodically whilst the apparatus 2 is switched on. As is conventional, the registration process takes the form of the broadcasting of a signal identifying the mobile terminal 2 (e.g. by transmitting its telephone number on a common hailing or signalling frequency).

The transmitted signal is picked up by one or more of the satellites 4. Under normal circumstances, the signal is picked up by multiple satellites 4, and the received signal strength and/or time of arrival are transmitted, together with the identity of the mobile apparatus 2 and the identity of the satellite 4 receiving the signal, to the database station 15 via the earth station node or nodes 6 for which the satellites 4 are in communication, and the signalling line 60.

The processor 58 of the database station 15 then calculates, e.g. on the basis of the differential arrival times, the terrestrial position of the mobile terminal apparatus 2, which is stored in the database 54. Also stored is the identity of the earth station node 6 most suitable for communicating with the mobile terminal apparatus 2 (the "active" station). This is typically found by the processor 58 comparing the stored position of the terminal 2 with the predetermined stored positions of each of the earth station nodes 6 and selecting the nearest. However, account may also or instead be taken of the strength of the signals received via the satellites 4, or of other factors such as network congestion, which may result, in borderline cases, in the choice of a node earth station which is not geographically closest to the mobile terminal equipment 2. The identity of the allocated active earth station node 6 is then likewise stored in the store 54 in the record for that terminal apparatus.

Call Set Up and Routing

The processes of routing calls to and from mobile terminal apparatus 2 are described fully in GB-A-2295296 and PCT/GB95/01087, both of which are hereby incorporated fully by reference. Briefly, for a local user outside its area, a call placed to the user or from the user is referred to the database station which determines that the user is outside of its area and thereafter does not process the call.

For a local user which is inside its area, in the preferred embodiment described in the above referenced British and International application, calls to or from the mobile user and a conventional terrestrial user connected to one of the PSTNs are set up over the satellite link, via the active earth station 6, the ground network, and the international public switch telephone network (PSTN) from the nearest gateway 8 to the terrestrial user.

For global users, calls are routed via the satellite and the active earth station, then via the ground network to the gateway station 8 nearest to the terrestrial user.

The dial numbers allocated to mobile users may have "International" prefixes followed by a code corresponding to the satellite service network. Alternatively, they could have a national prefix followed by a regional code assigned to the satellite service.

Calls between one mobile user and another are carried out by directing the signal via a first satellite link down to the active earth station node of the first mobile user, via the ground network to the active earth station node of the second mobile user (which may be, but is not necessarily, the same as that of the first) and then via a second satellite link (which may, but does not need to be via the same satellite) to the second mobile user.

First Embodiment

Figure 8 shows in greater detail the signal flow through the elements of the

mobile terminal of Figure 2. Signals received from the aerial 31 are RF demodulated by RF modem 32 and supplied to the processor circuit 37 which is arranged, when in enciphering mode, to decipher the received data using, for example, the A5 algorithm in accordance with a deciphering key supplied from the SIM 35. The deciphering key is referred to as $K_{a,b}$.

The deciphered bit stream is then passed to a channel codec 30b which performs error correcting decoding and the error corrected speech signal is supplied to low bit rate codec 30a which includes a digital to analog converter, the analog output of which is supplied to loudspeaker 34.

Speech from the microphone 36 is supplied to the low bit rate codec 30a which includes an analog to digital converter, and the resulting low bit rate speech signal is encoded by the channel codec 30b to include error protection. The error protected bit stream is then encrypted, when in enciphering mode, by the control circuit 37 and the encrypted bit stream is supplied to the RF modem 32 for transmission from the aerial 31.

Referring to Figures 9, 10 and 11, the process of setting up the enciphered mode of communication will now be described in greater detail.

During a communication session between two user terminals 2a,2b, a user of one or both terminals elects to continue the conversation in encrypted form. Accordingly, referring to Figure 10, in step 1002 the invoking party enters a sequence of key strokes from the keyboard 38, or operates on a special key which is recognised by the processor 37 as an instruction to invoke security, and accordingly the processor 37 transmits, in step 1002, a signal to invoke enciphering on an inband or associated control channel.

Referring to Figure 11, at the earth station 6, in step 1102 the privacy request signal is received and in step 1104 the signal is sent to the central database station 15 together with the identity codes indicating the identities of the

terminals 2a and 2b, and to the second user terminal 2b.

At the second user terminal 2b, receipt of the privacy signal occurs in step 1002 of Figure 10.

Referring to Figure 12, at the central database station the privacy signal is received in step 1202.

In step 1204, the controller 58 of the database station 15 accesses the memory 54 and reads out the individual enciphering key K_a stored for the first mobile terminal 2a, and the key K_b stored for the second mobile terminal 2b.

In step 1206, the controller 58 generates a pseudo random number (RAND).

In this embodiment, the keys K_a and K_b are each 128 bit binary numbers and the random number RAND is another 128 bit binary number.

In step 1208, the controller 58 calculates first and second partial keys K_a, K_{pb}. The calculation of the first partial key is illustrated in Figure 15; this calculation comprises generating a 128 bit number each bit of which comprises the exclusive OR function of the bits in corresponding positions of the second terminal key K_a and the random number RAND. Thus, the second partial key is given as follows

$K_{pa} = K_a + RAND$

(where + indicates a binary addition operation).

The second partial key K_{pb} is calculated in exactly the same way, by performing a bit-wise exclusive-OR operation between the first terminal key K_b and the random number RAND, as shown in Figure 15.

In step 1210 of Figure 12, the central database station 15 transmits the first partial key (K_{pa}), to the first terminal 2a and the second partial key (K_{pb}) to

the first terminal 2b, via the signalling network 60, and the respective earth stations 6b and 6a and satellites 4b and 4a.

At this stage, each individual terminal key has been "scrambled" by the binary addition operation with the random number RAND. An unauthorised eavesdropper who monitors one of the partial keys cannot learn the terminal key from it because there are two unknowns; the random number RAND and the terminal key. Even an unauthorised eavesdropper who monitors both partial keys cannot derive either the random number or one of the terminal keys, because he has only two data from which to derive three unknowns; the best that can be derived is the difference between the two terminal keys, which is of no value.

Referring now to Figure 11, in step 1106 each earth station receives the partial key and forwards it to the mobile terminal in step 1108.

Referring to Figure 10, in step 1004, each of the mobile terminals (2a, 2b) receives a corresponding partial key (K_{pa}, K_{pb}). In step 1006, the partial key is transmitted via the card reader 33 to the SIM 35.

Referring to Figure 13, in step 1302, the SIM receives the partial key and in step 1304 the SIM reads the terminal key from within the memory 35b. In step 1306, the SIM processor 35a recovers the binary number RAND by comparing the stored terminal key K_a from the partial key K_{pa}, to generate a new 128 bit binary number. The comparing step is carried out by exclusive-ORing K_{pa} and K_a. Thus, the SIM processor computes a code K_R where

$K_R = K_{pa}$

$= K_a + (RAND) - K_a$

$= (RAND)$

In step 1308, the SIM 35 supplies $K_R = (RAND)$ the card reader device 33 to the terminal processor 37. The code K_R is used as an enciphering key for data to be transmitted.

Likewise, at the second terminal 2b, the value of K_R = (RAND) is computed by subtracting the stored value Kb in the SIM of the terminal from the second partial key K_{pb}, i.e.

$K_R = K_{pb} - K_b$

$= Kb + (RAND) - K_b$

$= (RAND)$

Thus, each terminal 2a, 2b, calculates the same enciphering key K_R = (RAND).

Referring back to Figure 10, in step 1008, the terminal processor 37 receives the encryption key K_R and in step 1010 the terminal 37 switches to encryption mode. Thereafter, at step 1012, the processor 37 functions to encrypt the bit stream from the codec 30 prior to RF modulation and transmission, and to decrypt the corresponding bit stream from the RF modem 32 prior to supply thereof to the codec 30 using the key K_R.

The encryption algorithm may be any suitable algorithm and may be openly known, since the encryption key K_R itself is secret. The encryption algorithm is conveniently the A5 encryption algorithm used in GSM handsets and described in the above referenced GSM Recommendations.

Thus, to recap, as shown in Figure 9, in this embodiment each terminal 2 has an associated unique terminal key which is stored in the SIM 35 held within the terminal and in the central database station 15. The enciphering key K_R used is a function of the random number (RAND) generated in the remote database station 15 which distributes it to 2a, 2b in a masked form, in the partial keys K_{pa}, K_{pb}.

Transmitting the terminal keys in masked form prevents an eavesdropper from gaining access to either terminal key. By changing the masking on each session operation namely by generating a continually changing sequence of pseudo-random numbers (RAND), an eavesdropper cannot learn the masking

function over time.

Nor is it possible for either terminal or SIM to work out the other's terminal key, since this is masked even from the terminals themselves.

Second Embodiment

In a second embodiment, security is further improved by reducing the opportunities for unauthorised tampering at the central database station. The second embodiment works substantially as the first except that, as shown in Figure 14, instead of steps 1204 to 1210 of Figure 12 being performed, steps 1404 to 1420 are performed.

Accordingly, after step 1202, the processor 58 first accesses the first terminal key K_a in step 1404, then calculates the random number in step 1406 (as described in relation to step 1206), then calculates the first partial key K_{pa} in step 1408 (as described in relation to step 1208),and then sends the first partial key in step 1410 (as described in relation to step 1210).

After these operations, any locally stored copies of K_a and K_{pa} are erased. Then, in step 1414, the processor 58 accesses the second terminal key Kb, calculates the second partial key K_{pb} (step 1416), sends the second partial key (step 1418), and erases the second partial key and second terminal key (step 1420).

Thus, in this embodiment, access to the two partial keys and terminal keys is separated in time, reducing the possibilities for eavesdropping or fraudulent use of the database station 15.

It will be apparent that access to the two partial keys and/or terminal keys could be separated in other ways; for example, by sending the two terminal keys to physically separate devices and then sending the random number to each of the devices for combination there with the terminal keys.

Rather than sending the same random number to two different devices, for additional security, two identical, in-step, random number generators may be provided at two different locations, to which the two terminal keys are sent. Thus, access to the two terminal keys and/or partial keys may be separated physically as well as, or instead of, in time.

Third Embodiment

In this embodiment, security is further increased by enciphering each of the partial keys K_{pa}, for transmission. Although it would be possible to use a common cipher, this would be undesirable since eavesdroppers with access to the common cipher (e.g. other authorised users of the privacy service) might be able decipher the cipher.

Equally, it is preferred not to use an air interface cipher of the type known in the GSM system because this would be open to interception in the fixed part of the network.

Accordingly, in this embodiment, the SIM 35 stores a decryption algorithm (which may conveniently be the A5 algorithm used in GSM systems) and the database station 15 is arranged to execute the corresponding encryption algorithm.

Referring to Figure 17a, in this embodiment the process of Figure 12 of the first embodiment is modified by the inclusion of a step 1209, between steps 1208 and 1210, in which each partial key is enciphered using the terminal key of the terminal to which it will be sent and is transmitted in enciphered form.

At each terminal, referring to Figure 17b, in this embodiment the SIM processor 35a performs an additional step 1305 between steps 1304 and 1306. In step 1305, the received partial key is decrypted using the terminal key, prior to calculating the ciphering key.

Thus, in this embodiment, additional security is provided by encrypting the transmitted partial keys and conveniently, the encryption makes use of the terminal key of the destination terminal, so to avoid the need to store further encryption data.

Obviously, however, other forms of encryption are possible; in particular, more sophisticated encryption algorithms in which an additional random number is also sent would be possible.

Fourth Embodiment

In this embodiment, the principle of the first embodiment is utilised, in combination with the air interface encipherment and authentication system presence in GSM compatible networks and specified in the above GSM recommendations.

Referring to Figure 14, the security features are applied in the following order:

Authentication (step 2002); Air-Interface encryption (step 2004); End-to-End encryption (step 2006).

The first two steps are as in existing GSM networks and the third is as described above as in relation to the first embodiment. The process will now be described in more detail.

Referring to Figure 19a, the functions performed by the handset processor 37 and SIM 35 will be described as separate functional blocks; each functional block could, of course, be implemented by a separate microprocessor or digital signal processor (DSP) device but in this embodiment, in fact, only one such processor device is present in the handset and one in the SAN 35.

Referring to Figure 19a, signals received from the antenna 31 and demodulated *by* the RF modem 32 are passed through a first enciphering/deciphering stage

372 arranged to apply the AS algorithm known from GSM in accordance with an air interface enciphering key K_c, and a second enciphering/deciphering stage 374 arranged to apply a second deciphering algorithm (conveniently, again, the A5 algorithm used in the GSM system and described in the above Recommendations) deciphering in accordance with an end-to-end enciphering key $K_{a,b}$. The deciphered bit stream is thereafter supplied to the codec 30.

Similarly, the speech bit stream from the codec 30 passes through the two enciphering/deciphering stages 372,374 in the reverse order; for clarity, the signal path has been omitted from Figure 19a.

Within the SIM 35 is located a terminal key storage register 352 storing the terminal key K_a for the terminal, in this case K_1 for the terminal 2a. The terminal key storage register 352 is connected to supply the terminal key K_a to a signature calculation stage 354, arranged to calculate a "signed response" number (SRES) used to authenticate the terminal, in accordance with the A3 algorithm described in the above mentioned GSM Recommendations and used in GSM systems. The response calculation stage 354 is also connected, via the card reader device 33, to receive a random number (RAND1) from the unenciphered bit stream output from the RF modem 32.

The terminal key register 352 is also connected to supply the terminal key K_a to a first key generation stage 356, which is also arranged to receive the random number (RAND1) and to calculate therefrom an air interface enciphering key Kc in accordance with the A8 algorithm described in the above GSM Recommendations and used in GSM systems. The key thus calculated is supplied, via the card reader device 33, to the first (air interface) enciphering/deciphering stage 372 of the terminal processor 37.

The terminal key register 352 is also connected to supply the terminal key to a second key generation stage 358, which is arranged to generate an enciphering key K_R for end-to-end encryption (by an exclusive OR function as

described in the first embodiment) utilising the terminal key K_i and the partial key K_{pa} which it is connected to receive (via the card reader device 33) from the deciphered output of the first (air interface) enciphering/deciphering stage 372 of the terminal processor 37.

The end-to-end enciphering key thus calculated is supplied to the second (end-to-end) enciphering/ deciphering stage 374 of the terminal processor 37.

Referring to Figure 15b, the central database station 15 comprises, in this embodiment, a random number generator 582 arranged to generate, on each occasion of use, a new binary 128 bit number (RAND1) in a random sequence; a store 54 storing the terminal keys K_i; a key generation stage 584 which is connected to receive a terminal key from the store 54, and the random number (RAND1), and to calculate therefrom an air interface enciphering key K_c in accordance with the A8 algorithm described in the GSM recommendations and used in GSM systems; and a signature calculation stage 586, which likewise is connected to receive the terminal key and the random number (RAND1), arranged to calculate the signed response number (SRES) in accordance with the A3 algorithm described in the above mentioned GSM Recommendation and used in GSM systems.

The outputs of the random number generator stage 582, signed response generator stage 586 and key generation stage 584 are connected to the signalling circuit 56 for transmission to the earth stations 6.

Referring to Figure 19c, each earth station 6 comprises (within the database 48) a triplet register 482 arranged to store a predetermined number (e.g. 5) of triplets each comprising a random number, a corresponding SRES and a corresponding air interface encryption key K_c, supplied via the signalling circuit 60 from the database station 15.

On each occasion when a mobile terminal 2 registers with the earth station 6,

the earth station requests the supply of the predetermined number of triplets from the central database station 15, which accordingly generates the predetermined number of triplets and transmits them for storage in the registers 482 via signalling channel 60.

Also provided within the earth station 6 is a comparator 282 coupled to the triplet register 482 and to the air interface components 24, 26 of the earth station 6, and arranged to compare a signed response (SRES) number received from a mobile terminal 2 with a signed response stored in the register 482, and to indicate correspondence (or absence thereof) between the two numbers. If the two numbers do not correspond, the user is not authenticated and service is discontinued by the control unit 28.

Finally, the earth station 6 comprises an air interface encryption stage 284 arranged to encipher and decipher in accordance with the A5 algorithm (known from GSM) making use of an air interface enciphering key K_c supplied from the triplet register 482.

In the enciphering direction, the air interface enciphering/deciphering stage 284 receives an input from the codec 50 (Figure 3) and delivers its output to the air interface components 24,26; whereas in the deciphering direction the enciphering/deciphering stage 284 receives its input from the air interface components 24, 26 and delivers its output to the codec 50.

The operation of this embodiment will now be described in greater detail with reference to Figures 16a to 16d. In Figures 20 to 23, steps of the processes of Figure 10 to 13, which will not be discussed further in detail, are incorporated.

As in Figure 10, a request for privacy is initiated by one of the parties and a privacy request signal is transmitted from the terminal 2a.

Following receipt (step 1102) of the privacy signal at the earth station 6a and forwarding thereof (step 1104) to the database station 15, referring to Figure 16c, steps 1202 and 1204 are performed to derive the terminal keys of the two terminals.

Then, in step 1205, a test is performed to determine whether both subscribers are authorised to use end-to-end encryption. If so, steps 1206 to 1210 of Figure 12 are performed. Subsequently, or if not, the database station 15 proceeds to step 1212, in which it transmits a signal to the earth station(s) 6a,6b serving the two terminals 2a,2b to instruct them to perform a terminal authentication check and to commence air interface encryption.

Referring back to Figure 21, each earth station 6, on receipt of the instruction signal and partial key (step 1110), sends an authentication interrogation message (step 1112) which includes the next random number RAND1 obtained from the triplet register 482. Additionally, as in the GSM system, a key number may be transmitted for further verification.

Referring back to Figure 20, on receipt of the authentication request message (step 1014) the random number (RANDI) is extracted and sent to the SIM 35 (step 1016).

Referring to Figure 16d, at the SIM 35, on receipt of the random number RAND1 (step 1310), the SIM processor 35a looks up the terminal key K_a, (step 1312) and calculates the signed response (SRES) using the A3 algorithm (step 1314).

In step 1316, the SIM processor 35a calculates the air interface enciphering key K_c using the random number (RAND1) and the terminal key K_a. In step 1318, the SIM 35 transmits the signed response number (SRES) and the air interface enciphering key (K_c) to the terminal processor 37 via the card reader device 33.

Subsequently, the SIM 35 executes the process of Figure 13.

Referring to Figure 20, on receipt of the signed response number (SRES) in step 1018, the terminal processor 37 transmits the SRES number to the earth station 6a (step 1020).

Referring to Figure 21, the earth station 6 receives the signed response number (1114) and compares it with the stored signed response number held in the triplet register 482 (step 1116).

If the two do not match, the call is terminated (step 1117). Alternatively, further attempts at authentication may be made if desired.

If the signed response received from the mobile terminal 2 matches the stored signed response in step 1116, the earth station 6 reads the enciphering key K_c stored in the triplet register 482 corresponding to the signed response just received, and (step 1118) commences enciphering all future traffic to, and deciphering all future traffic from, the mobile terminal 2 using the AS algorithm together with the enciphering key K_c. As is conventional in GSM systems, the frame number may also be used as an input to the enciphering algorithm.

The earth station 6 thereafter returns to step 1108 of Figure 11, to send the partial key K_{pa} received from the database station 15 to the terminal 2a, but in this embodiment this takes place in enciphered form.

Returning to Figure 16a, on receipt of the air interface encryption key K_c (step 1022) from the SIM 35, the terminal processor 37 starts the enciphering/deciphering mode in which all traffic received from the air interface modem 32 is deciphered and all traffic transmitted to the air interface modem 32 is enciphered using the A5 algorithm and the air interface enciphering key Kc; where the earth station 6 additionally makes use of the frame number, the

terminal 2 likewise does so.

The process performed by the terminal processor 37 of terminal 2a (in this example) then returns to step 1004 of Figure 10, to receive (in encrypted form), decrypt and use the partial enciphering key K_{pa} received from the earth station 6. A corresponding process is performed for the terminal 2b.

Although the above description assumes that neither terminal has recently been authenticated, and that neither terminal is already in air interface encryption mode, it will be understood that this need not be the case. If either terminal is already applying air interface encryption, then the corresponding steps described above to set up authentication and air interface enciphering are not performed again.

In the above embodiment, additional safeguards may be provided; for example, to initiate secure communications, the terminal user may be required to input a PIN code for matching with data held on the SIM.

It will be understood that, where the invention is practised in a GSM-compatible system or the like, the SIM 35 will contain further information in the form of the international mobile subscriber identity number (IMSI), and optionally lists of phone numbers for speed dial or other purposes.

Conference Calls

The encryption scheme according to the invention has the significant advantage that the common encryption/decryption code K_R that is formed in each of the terminals 2a, 2b consists of the random number (RAND) supplied from the data base station 15. Thus, in the method according to the invention, the length of the encryption/decryption code K_R is independent of the number of terminals used during the call. This has implications for conference calls as will now be explained with reference to Figure 24. This Figure corresponds generally to Figure 9 but illustrates more than two user

terminals, for use in a conference call. In Figure 24, three terminals are shown, namely terminal 2a, 2b and 2n which each form a respective communication link with a earth station 6a, 6b, and 6n.

In order to set up the conference call, partial keys K_{pa}, K_{pb} and K_{pn} are transmitted from the central database station 15 to each of the earth stations 6a, 6b and 6n and the keys are then transmitted to the respective user terminals 2a, 2b, 2n. The partial keys are then decoded at the user terminals respectively in the manner previously described such that each terminal develops the common encryption code K_R = (RAND). The terminals can then use the common code K_R to encrypt and decrypt data for the conference call between the three user terminals. It will be appreciated that although three terminals are shown, much larger numbers could be used for the conference call. This contrasts with the method described in our prior GB 9611411.1 in which each terminal needs to be provided with data based on the terminal key codes for all the other terminals used for the call and so when many terminals are used in a conference call, the encryption code becomes extremely long and cumbersome.

One or more additional terminals may join in a call whilst it is in progress, either to expand a normal two party call into a three party conference call or to increase the number of parties in a conference call. To this end, the joining party is sent a masked version of the code RAND from the base station 15 together with the frame number for the data transmission that is going on between the parties, so that the joining party can use the locally held A5 algorithm to compute the current value of the encryption key and join in the transmitted data flow .

The ability to set up secure conference calls between many user terminals has particular application for secure closed user group (CUG). To this end, the database station 15 may include a list of members of a closed user group which are permitted to correspond with other members in a conference call or

individually. For example, a closed user group may comprise armed services personnel or emergency services personnel. In a modification, more than one database station 15 is provided and a supervising database station (not shown) may be used to in order to coordinate more than one CUG to allow them to share facilities, for example on a temporary basis so that for a particular project e.g. a combined service operation, the CUGs may communication with each other over conference calls or individually in a secure, encrypted manner. In another modification, a single database station 15 is used and, for the temporary period of cooperation, all user terminals are provided with reprogrammed SIM cards to allow secure communication within the temporary group.

Other Embodiments

Many modifications and alternative to the previously described embodiments will be apparent to the skilled person and are within the scope of the present invention.

For example, in practice, duplex transmission occurs between, the user terminals on different channels. For additional security different individual codes K_R, may be used for each of the duplex channels, produced by means of separate partial keys transmitted from the database station 15, using different values of the pseudo random number (RAND) for each channel.

The numbers of satellites and satellite orbits indicated are purely exemplary. Smaller numbers of geostationary satellites, or satellites in higher altitude orbits, could be used; or larger numbers of low earth orbit (LEO) satellites could be used. Equally, different numbers of satellites in intermediate orbits could be used.

Although TDMA has been mentioned as suitable access protocol, other access protocols can be used such as code division multiple access (CDMA) or frequency division multiple access (FDMA).

Whilst the principles of the present invention are envisaged above as being applied to satellite communication systems, the use of the invention in other communications systems e.g. digital terrestrial cellular systems such as, but not limited to GSM, is also possible.

Although, for the sake of convenience, the term "mobile" has been used in the foregoing description to denote the terminals 2, it should be understood that this term is not restricted to hand-held or handportable terminals, but includes, for example, terminals to be mounted on marine vessels or aircraft, or in terrestrial vehicles. Equally, it is possible to practice the invention with some of the terminals 2 being completely immobile.

Instead of providing a single central database station 15 storing details of all terminal equipment 2, similar details could be stored at the home gateway 8 for all terminal equipment to register with that home gateway 8.

Whilst in the above described embodiments the central database station 15 acts as a Home Location Register (HLR) of a GSM system, and may be provided using commercially available HLR hardware, and the databases within each earth station 6 act in the manner of visiting location registers (VLRs) and may likewise use commercially available GSM hardware, it will be understood that the information relating to different users could be distributed between several different databases. There could, for instance, be one database for each closed user group, at physically different positions.

Whilst in the fourth embodiment above the same terminal key K_i is used for secure end-to-end encryption as is used for air interface encryption, it will be clear that this is not necessary; each terminal could store two different terminal keys, one for air interface encryption and one for end-to-end encryption. In this case, a separate authentication centre database could be provided for end-to-end encryption key distribution to that which is used in conventional air interface encryption.

Although in the foregoing embodiments, the same (AS) cipher algorithm used for the air interface encryption of the GSM system is used in end-to-end encryption, it will be apparent that a different cipher could be used; in this case, terminals would include two different enciphering stages for use in the fourth embodiment. Further, where multiple closed user groups are provided, each closed user group could use a different cipher.

In the foregoing, the gateways 8 may in fact be comprised within an ISC or exchange or mobile switching centre (MSC) by providing additional operating control programmes performing the function of the gateway.

In the foregoing, dedicated ground networks lines have been described, and are preferred. However, use of PSTN or PLMN links is not excluded where, for example, leased lines are unavailable or where temporary additional capacity is required to cope with traffic conditions.

It will understood that the stores within the gateways 8 need not be physically co-located with other components thereof, provided they are connected via a signalling link.

Whilst, in the foregoing, the term "global" is used, and it is preferred that the satellite system should cover all or a substantial part of the globe, the invention extends also to similar systems with more restricted coverage (for example of one or more continents).

Whilst the foregoing embodiments describe duplex communications systems, it will be clear that the invention is equally applicable to simplex (one way) transmission systems such as point-to-multipoint or broadcast systems.

Whilst the preceding, described embodiments are direct transmission systems, it will understood that the invention is applicable to store-and-forward communications systems in which one party transmits a message for storage

and subsequent later transmission to the other party.

One example of such a store-and-forward system is e-mail, for example of the type provided by Compuserve™ or MCI™. Another example is the Internet, which, as is well known, consists of a number of host computer sites interconnected by a backbone of high speed packet transmission links, and accessible for file transfer from most points in the world via public telecommunications or other networks.

In an embodiment of this type, a central database station 15 need not distribute keys to both terminals at the same time; instead, distribution of the partial key to the transmitting terminal may take place at the time of transmission of a file of data for storage in encrypted form, and distribution of a partial key to the receiving terminal may take place substantially later, for example, at the next occasion when the receiving terminal is connected to the network and/or the next occasion when the receiving terminal wishes download the file from intermediate storage in a host computer.

It will be understood that whilst the previously described embodiments concern voice transmission, the invention is applicable to the encryption of data of any kind and particularly, but not exclusively, to image data, video data, text files or the like.

It will be understood that the geographical locations of the various components of the invention are not important, and that different parts of the system of the above embodiments may be provided in different national jurisdictions and the present invention extends to any part or component of telecommunications apparatus or system which contributes to the inventive concept.

「以下余白」

4 Brief Description of Drawings

Figure 1 is a block diagram showing schematically the elements of a communication system embodying the present invention;

Figure 2 is a block diagram showing schematically the elements of mobile terminal equipment suitable for use with the present invention;

Figure 3 is a block diagram showing schematically the elements of an Earth station node forming part of the embodiment of Figure 1;

Figure 4 is a block diagram showing schematically the elements of a gateway station forming part of the embodiment of Figure 1;

Figure 5 is a block diagram showing schematically the elements of a database station forming part of the embodiment of Figure 1;

Figure 6 illustrates the contents of a store forming part of the database station of Figure 5;

Figure 7a illustrates schematically the beams produced by a satellite in the embodiment of Figure 1;

Figure 7b illustrates schematically the disposition of satellites forming part of Figure 1 in orbits around the earth;

Figure 8 is a block diagram showing the signal flow between components of the handset of Figure 2 in a first embodiment of the invention;

Figure 9 is a schematic block diagram showing the flow of encryption data and signals between the components of Figure 1 in the first embodiment;

Figure 10 is a flow diagram showing schematically the process performed by the control and enciphering components of the handset of Figure 8 in the first embodiment;

「以下 余白」

Figure 11 is a flow diagram showing schematically the process of operation of the earth station of Figure 3 in the first embodiment,

Figure 12 is a flow diagram showing schematically the process of operation of the central database station of Figure 4 in the first embodiment;

Figure 13 is a flow diagram showing schematically the process of operation of a subscriber information module (SIM) held within the handset of Figure 8 in the first embodiment;

Figure 14 is a flow diagram illustrating schematically the stages of security provided in a fourth embodiment of the invention;

Figure 15 is a an illustrative diagram showing the stages of formation of the enciphering key by a first handset terminal of Figure 8; and

Figure 16 is a corresponding illustrative diagram showing the process of formation of the enciphering key at a second such handset;

Figures 17a and b is a flow diagram modifying the operation of that of Figures 12 and 13 in the third embodiment of the invention;

Figure 19a is a block diagram showing schematically some of the functional elements present in the handset of Figure 8 according to the fourth embodiment of the invention;

Figure 19b is a block diagram showing schematically some of the functional elements present in the database station of the fourth embodiment,

Figure 19c is a block diagram showing schematically some of the functional elements present in the earth station of the fourth embodiment;

Figure 20 (incorporating parts of Figure 10) is a flow diagram showing schematically the operation of a handset according to the fourth embodiment;

Figure 21 (incorporating parts of Figure 11) is a flow diagram showing schematically the process of operation of an earth station according to the fourth embodiment;

Figure 22 (incorporating parts of Figure 12) is a flow diagram showing schematically the operation of a database station according to the fourth embodiment;

Figure 23 (incorporating parts of Figure 13) is a flow diagram showing schematically the operation of a subscriber information module according to

the fourth embodiment; and

Figure 24 illustrates how embodiments of the invention can be used for conference calls with more than two user terminals.

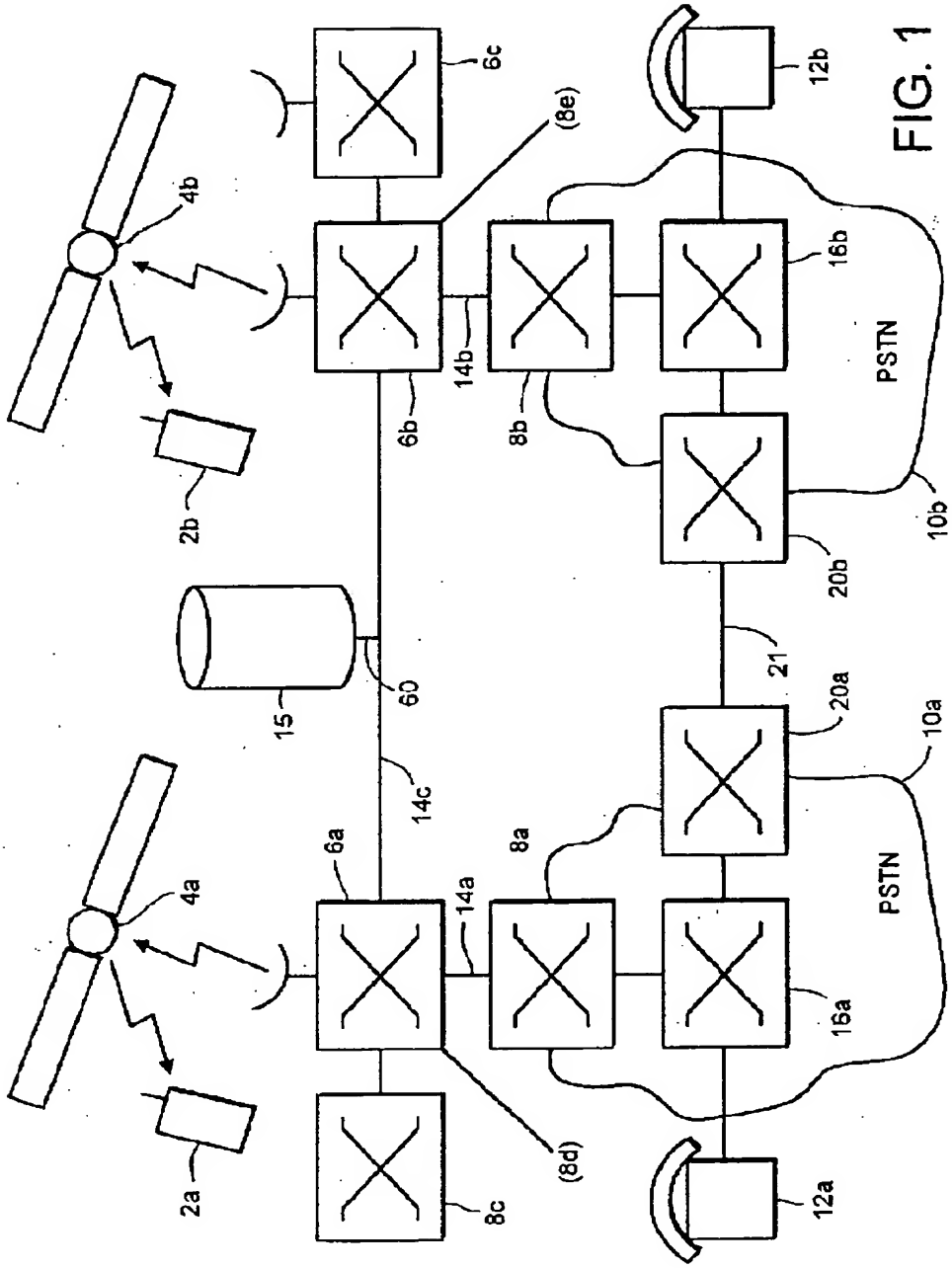
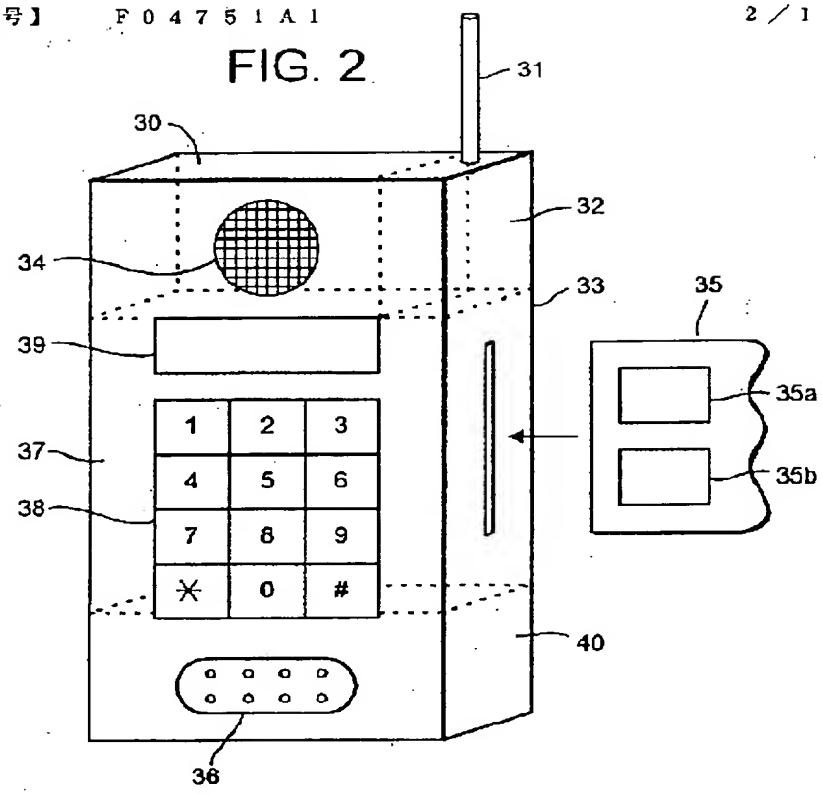

6c
(8e)
12b
4b
16b
PSTN
14b
6b
8b
2b
10b
20b
21
15
60
20a
10a
14c
6a
8a
4a
14a
PSTN
16a
(8d)
2a
8c
12a

FIG. 1

FIG. 2


31
30
32
34
33
35
39
35a
35b
1
2
3
37
4
5
6
38
7
8
9
*
0
#
40
36

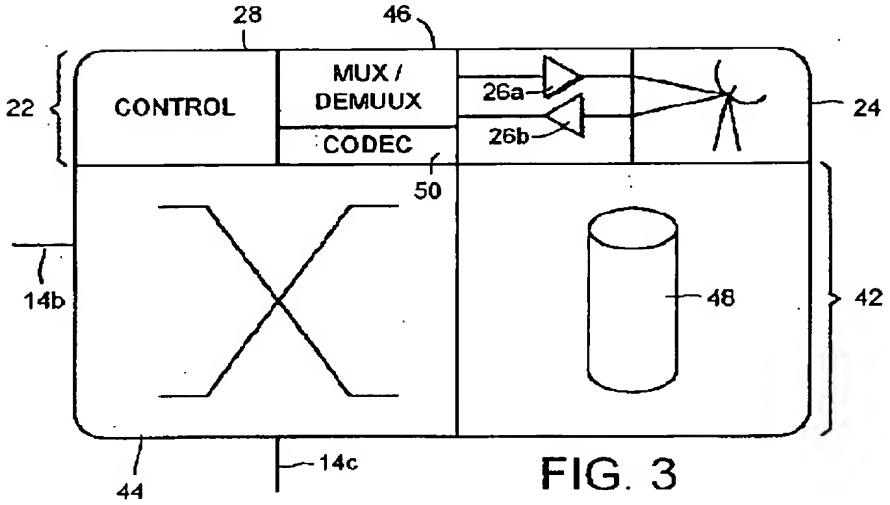

28
46
22
CONTROL
MUX / DEMUUX
CODEC
26a
26b
24
50
14b
48
42
44
14c

FIG. 3

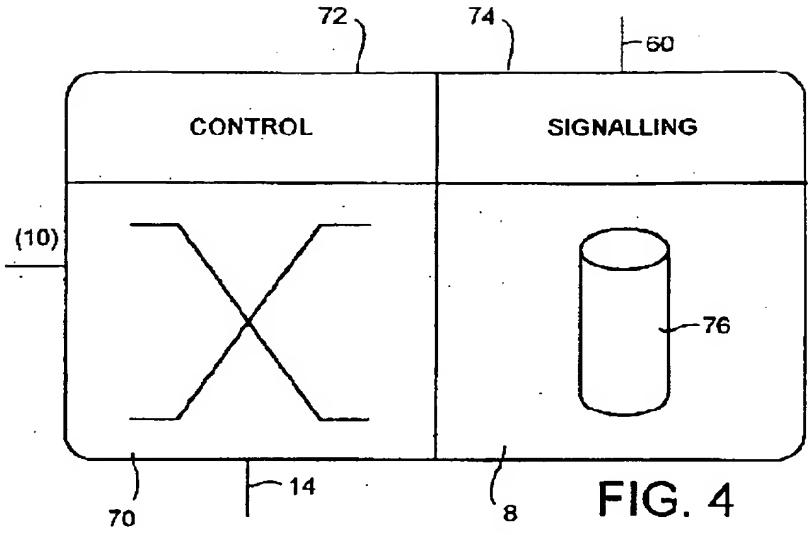

72
74
60
CONTROL
SIGNALLING
(10)
76
70
14
8

FIG. 4

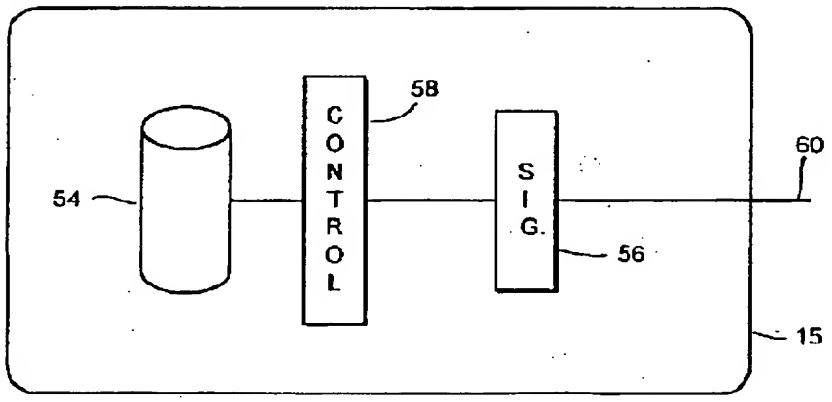

58
C
O
N
T
R
O
L
S
I
G.
54
60
56
15

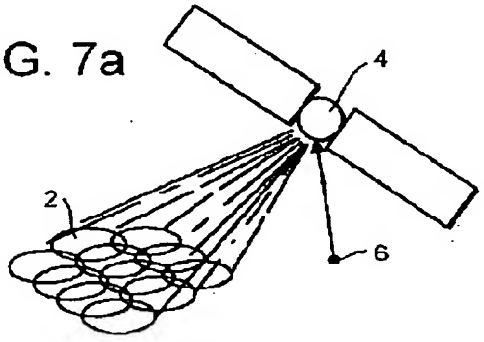
FIG. 5

54

ID #	KEY Ki	STATUS	POSITION	ACTIV NODE	AVAIL ?	HOME
00001	K_A	LOCAL	46°, 35°	6a	Y	8a
00002	K_B	GLOBAL	71°, 27°	6b	Y	8b

FIG. 6

FIG. 7a



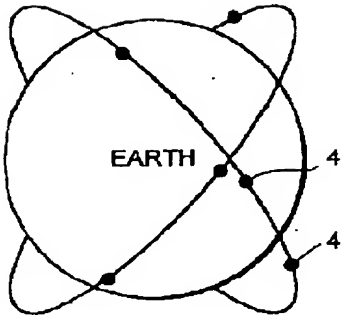


FIG. 7b

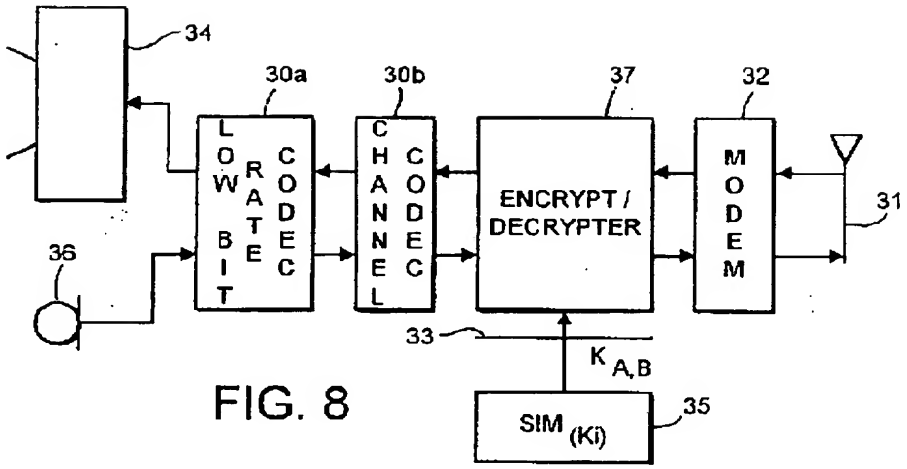

34
30a
30b
37
32
LOW BIT RATE CODEC
CHANNEL CODEC
ENCRYPT / DECRYPTER
MODEM
31
36
33
$K_{A,B}$
SIM (Ki)
35

FIG. 8

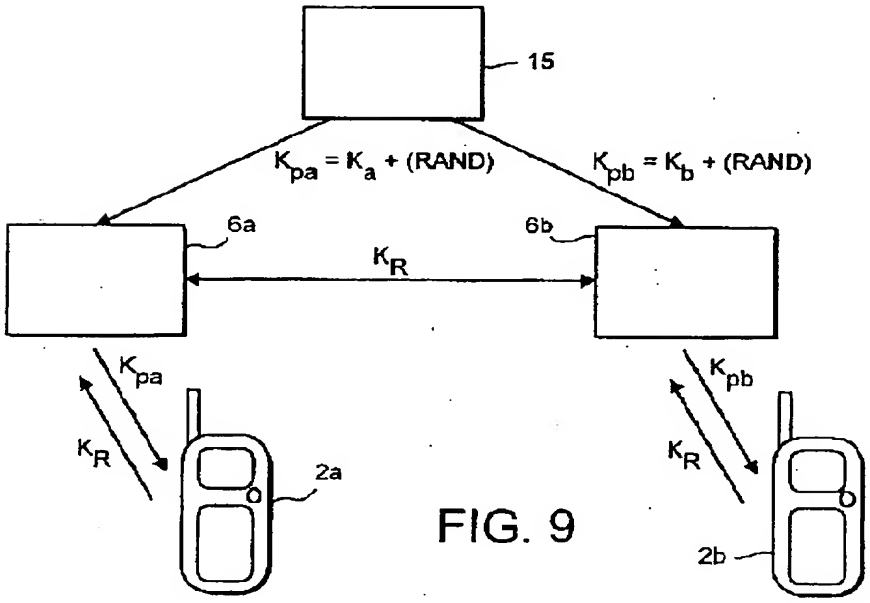

15
$K_{pa} = K_a + (RAND)$
$K_{pb} = K_b + (RAND)$
6a
6b
K_R
K_{pa}
K_R
K_{pb}
K_R
2a
2b

FIG. 9

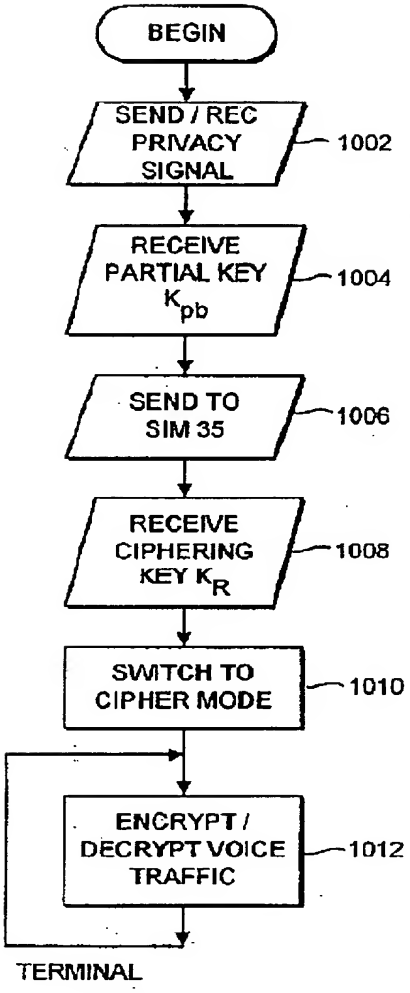

BEGIN
SEND / REC PRIVACY SIGNAL
1002
RECEIVE PARTIAL KEY K_{pb}
1004
SEND TO SIM 35
1006
RECEIVE CIPHERING KEY K_R
1008
SWITCH TO CIPHER MODE
1010
ENCRYPT / DECRYPT VOICE TRAFFIC
1012
TERMINAL

FIG. 10

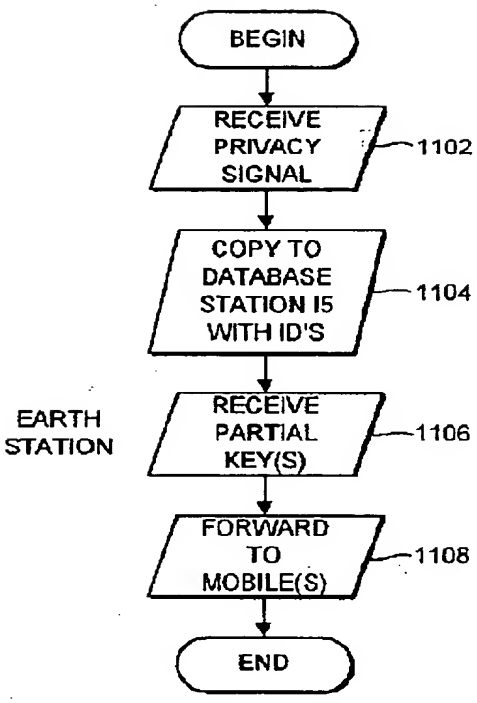

EARTH STATION
BEGIN
RECEIVE PRIVACY SIGNAL
1102
COPY TO DATABASE STATION I5 WITH ID'S
1104
RECEIVE PARTIAL KEY(S)
1106
FORWARD TO MOBILE(S)
1108
END

FIG. 11

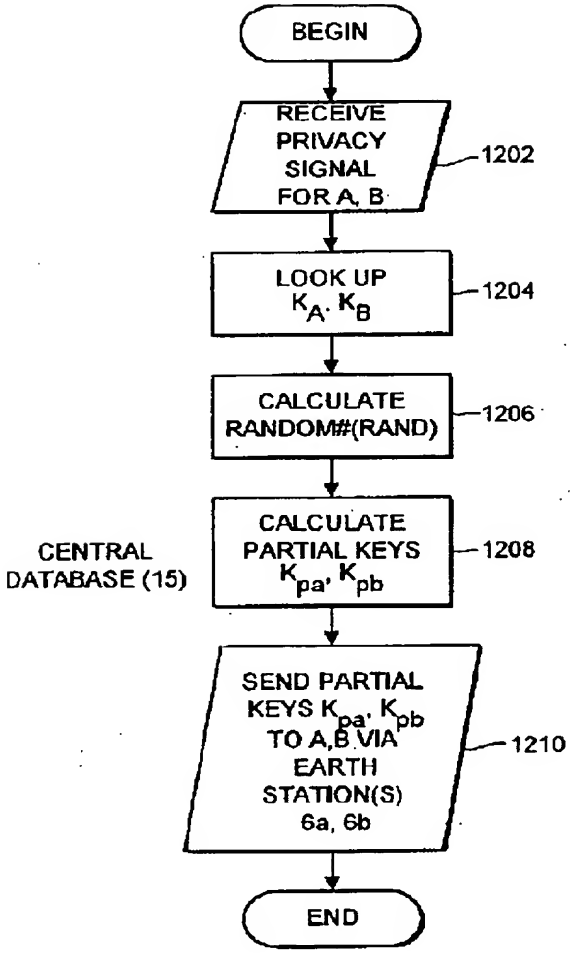

BEGIN
RECEIVE PRIVACY SIGNAL FOR A, B
1202
LOOK UP K_A, K_B
1204
CALCULATE RANDOM#(RAND)
1206
CENTRAL DATABASE (15)
CALCULATE PARTIAL KEYS K_{pa}, K_{pb}
1208
SEND PARTIAL KEYS K_{pa}, K_{pb} TO A,B VIA EARTH STATION(S) 6a, 6b
1210
END

FIG. 12

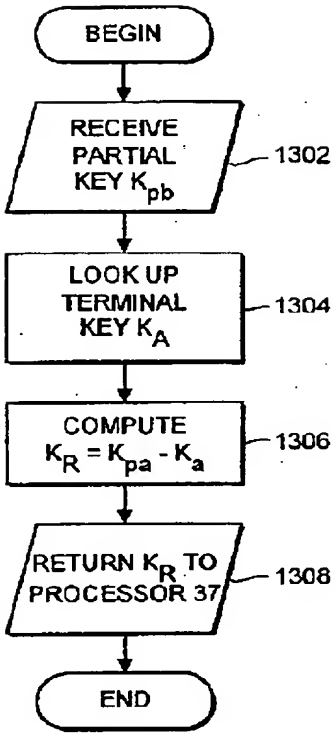

BEGIN
RECEIVE PARTIAL KEY K_{pb}
1302
LOOK UP TERMINAL KEY K_A
1304
COMPUTE $K_R = K_{pa} - K_a$
1306
RETURN K_R TO PROCESSOR 37
1308
END

FIG. 13

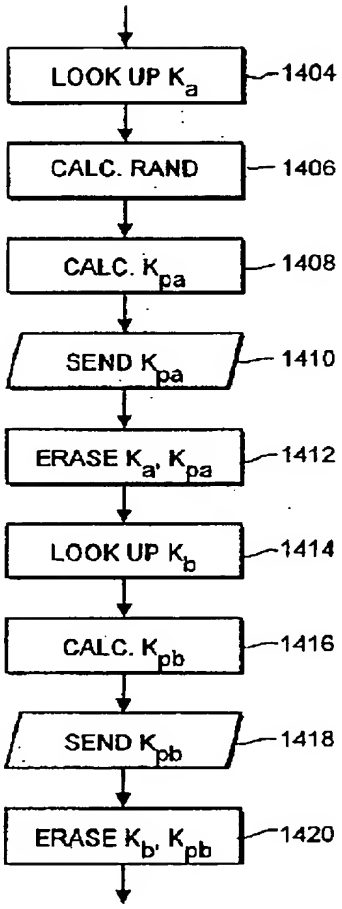


FIG. 14

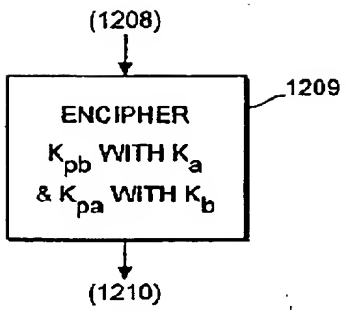


FIG. 17a

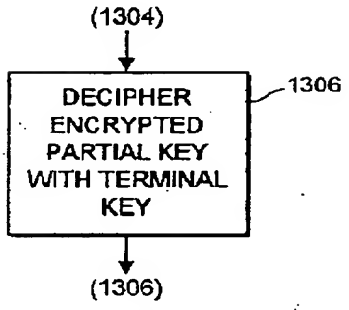


FIG. 17b

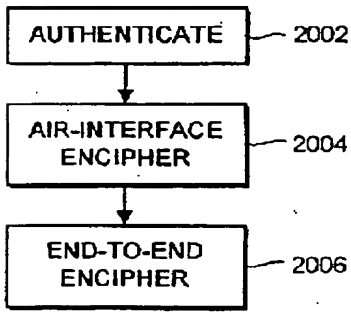


FIG. 18

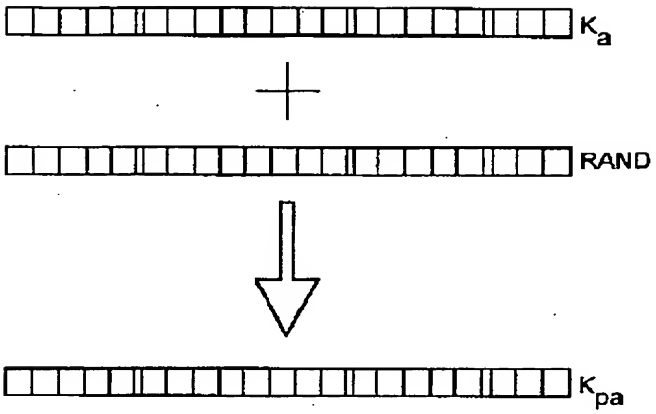


FIG. 15

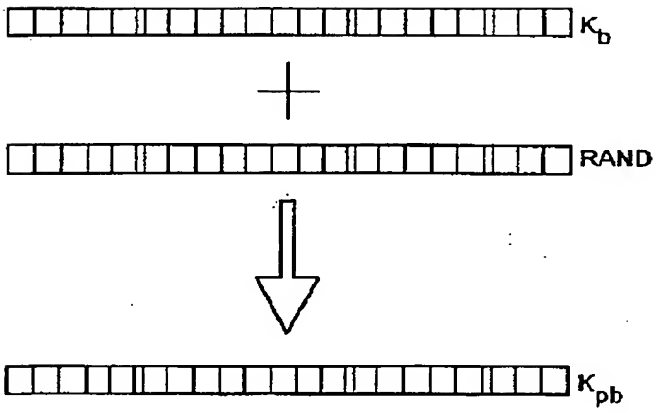


FIG. 16

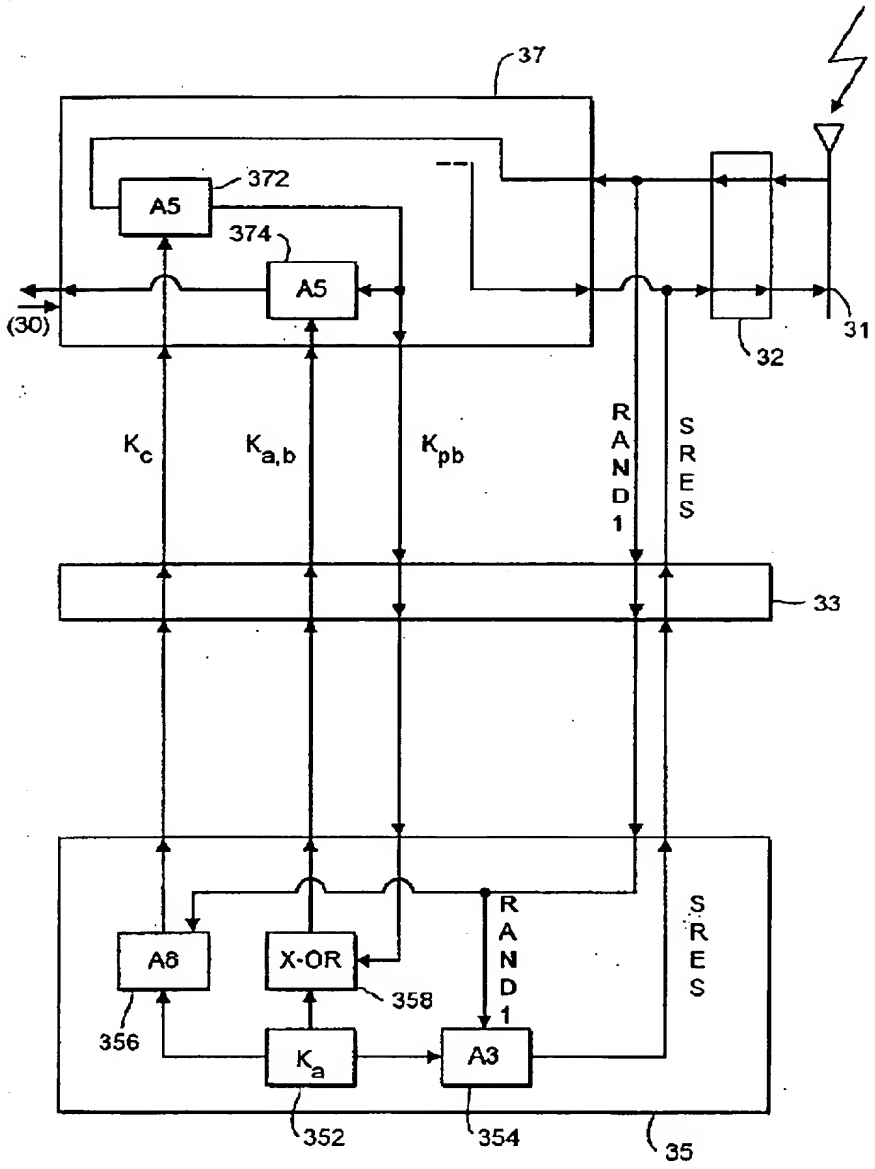

37
372
A5
374
A5
(30)
31
32
K_c
$K_{a,b}$
K_{pb}
RAND1
SRES
33
A8
X-OR
358
RAND1
SRES
356
K_a
A3
352
354
35

FIG. 19a

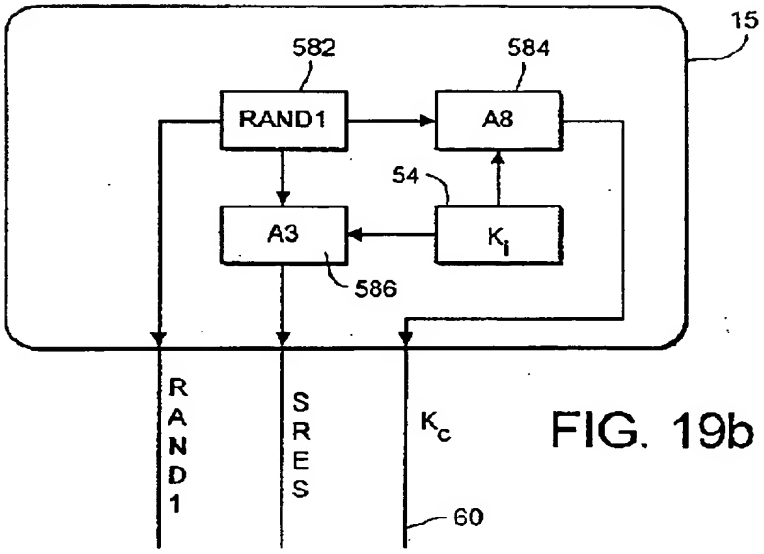


FIG. 19b

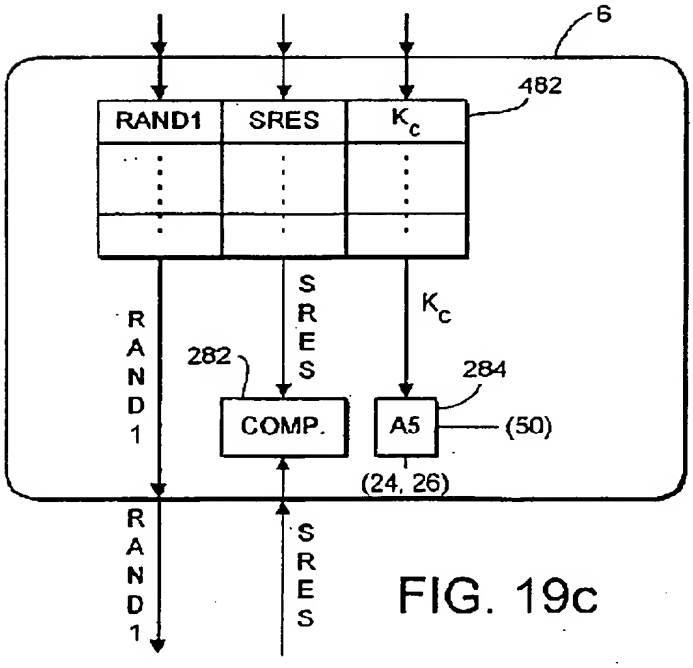


FIG. 19c

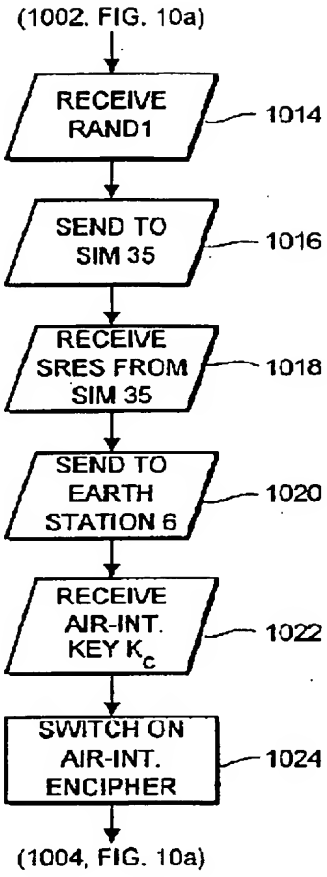

(1002. FIG. 10a)
RECEIVE RAND1
1014
SEND TO SIM 35
1016
RECEIVE SRES FROM SIM 35
1018
SEND TO EARTH STATION 6
1020
RECEIVE AIR-INT. KEY K_c
1022
SWITCH ON AIR-INT. ENCIPHER
1024
(1004, FIG. 10a)

FIG. 20

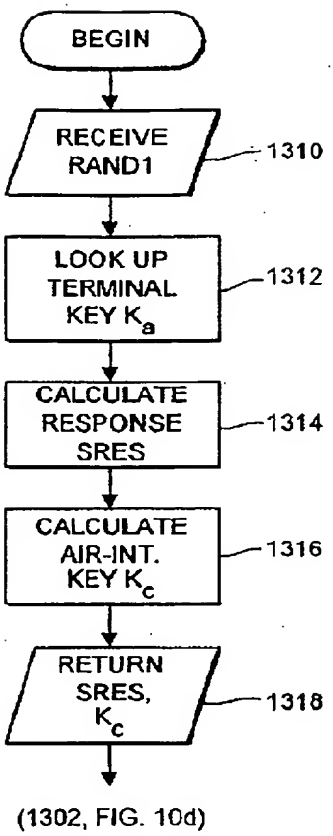

BEGIN
RECEIVE RAND1
1310
LOOK UP TERMINAL KEY K_a
1312
CALCULATE RESPONSE SRES
1314
CALCULATE AIR-INT. KEY K_c
1316
RETURN SRES, K_c
1318
(1302, FIG. 10d)

FIG. 23

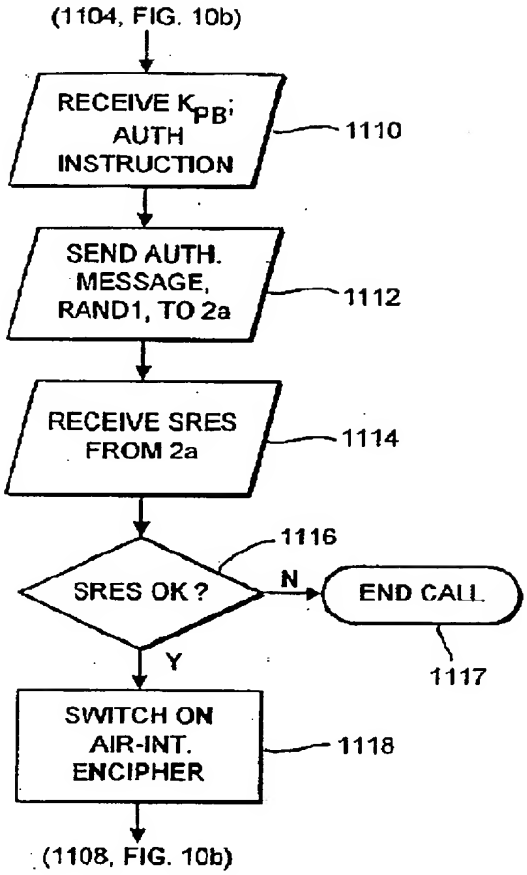

(1104, FIG. 10b)
RECEIVE K_{PB}, AUTH INSTRUCTION
1110
SEND AUTH. MESSAGE, RAND1, TO 2a
1112
RECEIVE SRES FROM 2a
1114
1116
SRES OK ?
N
END CALL
1117
Y
SWITCH ON AIR-INT. ENCIPHER
1118
(1108, FIG. 10b)

FIG. 21

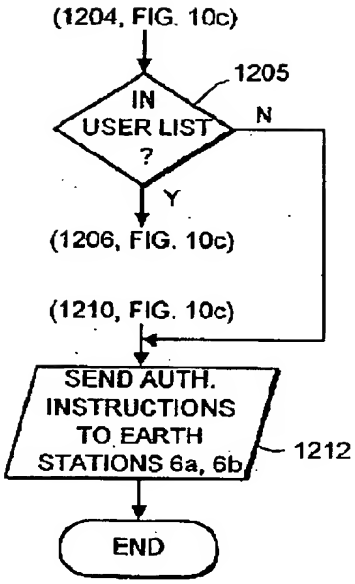

(1204, FIG. 10c)
1205
IN USER LIST ?
N
Y
(1206, FIG. 10c)
(1210, FIG. 10c)
SEND AUTH. INSTRUCTIONS TO EARTH STATIONS 6a, 6b
1212
END

FIG. 22

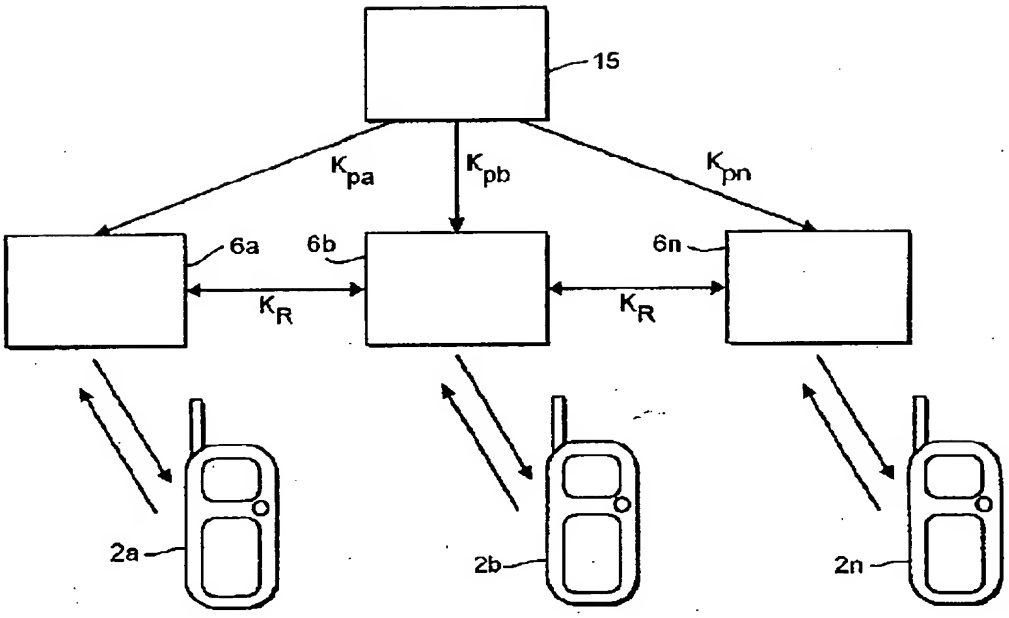


FIG. 24

1 Abstract

A satellite mobile telecommunications system includes mobile terminals 2a, 2b which can communicate with one another using end-to end encryption and decryption techniques. When secure end-to-end communication is required, each terminal uses a common encryption code (RAND) to encode data and decode data transmitted between the terminals. The encryption code is transmitted in a secure manner from a remote database station (15) to the terminals. Each terminal stores a terminal key (K_a, K_b) on its SIM card and the keys are also held in the remote station (15). Partial keys (K_{pa}, K_b) comprising the pseudo random number (RAND) and the keys K_a, K_b stored at the station (15) are produced at the station (15) by an exclusive OR process in order to mask the keys and the random number. The partial key $K_{pa} = K_a + (RAND)$ is sent to terminal 2a. At the terminal 2a, the partial key K_{pa} is exclusive OR-ed with the locally stored terminal key K_a on the SIM card, so as to recover (RAND). The common code (RAND) is determined by the same process at terminal 2b, from $K_{pb} = K_b + (RAND)$ and the locally stored key K_b. The terminals then both run a GSM encryption algorithm (A5) to encrypt and decrypt transmitted data, on the basis of the common code (RAND).

2 Representative Drawing

Fig. 1